

Safety Manager Software Reference

EP-SM.MAN.6285

Issue 1

20 February 2008

Release 131

| Document | Release | Issue | Date |
|----------------|---------|-------|---------------|
| EP-SM.MAN.6285 | 131 | 1 | February 2008 |

Notice

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell Safety Management Systems.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright 2008 – Honeywell Safety Management Systems, a division of Honeywell Aerospace B.V.

Honeywell trademarks

Experion PKS[®], PlantScape[®], SafeBrowse[®], TotalPlant[®] and TDC 3000[®] are U.S. registered trademarks of Honeywell International Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Support and other contacts

United States and Canada

Contact: Honeywell Solution Support Center
Phone: 1-800 822-7673. In Arizona: (602) 313-5558
Calls are answered by dispatcher between 6:00 am and 4:00 pm Mountain Standard Time. Emergency calls outside normal working hours are received by an answering service and returned within one hour.
Facsimile: (602) 313-3293
Mail: Honeywell IS TAC, MS P13
2500 West Union Hills Drive
Phoenix, AZ, 85027

Europe

Contact: Honeywell PACE TAC
Phone: +32-2-728-2657
Facsimile: +32-2-728-2278
Mail: Honeywell TAC BE02
Hermes Plaza
Hermeslaan, 1H
B-1831 Diegem, Belgium

Pacific

Contact: Honeywell Global TAC - Pacific
Phone: 1300-300-4822 (toll free within Australia)
+61-2-9362-9559 (outside Australia)
Facsimile: +61-2-9362-9564
Mail: Honeywell Limited Australia
5 Kitchener Way
Burswood 6100, Western Australia
Email GTAC@honeywell.com

India

Contact: Honeywell Global TAC - India
Phone: +91 20 6603 2718 / 19 and 1800 233 5051
Facsimile: +91-20-66039800
Mail: Honeywell Automation India Ltd.
56 and 57, Hadapsar Industrial Estate
Hadapsar, Pune –411 013, India
Email Global-TAC-India@honeywell.com

Korea

Contact: Honeywell Global TAC - Korea
Phone: +82-2-799-6317
+82-11-9227-6324
Facsimile: +82-2-792-9015
Mail: Honeywell Co., Ltd
17F, Kikje Center B/D,
191, Hangangro-2Ga
Yongsan-gu, Seoul, 140-702, Korea
Email Global-TAC-Korea@honeywell.com

People's Republic of China

Contact: Honeywell Global TAC - China
Phone: +86- 21-52574568
Mail: Honeywell (China) Co., Ltd
33/F, Tower A, City Center, 100 Zunyi Rd.
Shanghai 200051, People's Republic of China
Email Global-TAC-China@honeywell.com

Singapore

Contact: Honeywell Global TAC - South East Asia
Phone: +65-6580-3500
Facsimile: +65-6580-3501
+65-6445-3033
Mail: Honeywell Private Limited
Honeywell Building
17, Changi Business Park Central 1
Singapore 486073
Email GTAC-SEA@honeywell.com

Taiwan

Contact: Honeywell Global TAC - Taiwan
Phone: +886-7-536 2567
Facsimile: +886-7-536 2039
Mail: Honeywell Taiwan Ltd.
17F-1, No. 260, Jhongshan 2nd Road.
Cianjhen District
Kaohsiung, Taiwan, ROC
Email Global-TAC-Taiwan@honeywell.com

Japan

Contact: Honeywell Global TAC - Japan
Phone: +81-3-6730-7160
Facsimile: +81-3-6730-7228
Mail: Honeywell K.K.
New Pier Takeshiba, South Tower Building,
20th Floor, 1-16-1 Kaigan, Minato-ku,
Tokyo 105-0022, Japan
Email Global-TAC-JapanJA25@honeywell.com

Elsewhere

Call your nearest Honeywell office.

World Wide Web

Honeywell Solution Support Online:

<http://www.honeywell.com/ps>.

Training classes

Honeywell holds technical training classes on Safety Manager. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see <http://www.automationcollege.com>.

Related Documentation

The following guides are available for Safety Manager.

The guide in front of you is *Software Reference*.

| Guide | Description |
|--|---|
| The <i>Overview Guide</i> | This guide describes the general knowledge required, the basic functions of, and the tasks related to Safety Manager. |
| The <i>Safety Manual</i> | This guide describes the specifications, design guidelines, and safety aspects related to Safety Manager. |
| The <i>Planning and Design Guide</i> | This guide describes the tasks related to planning and designing a Safety Manager project. |
| The <i>Installation and Upgrade Guide</i> | This guide describes the tasks related to installing, replacing and upgrading hardware and software as part of a Safety Manager project. |
| The <i>Troubleshooting and Maintenance Guide</i> | This guide describes the tasks related to troubleshooting and maintaining Safety Manager. |
| The <i>System Administration Guide</i> | This guide describes the task related to administrating the computer systems used in a Safety Manager project. |
| The <i>Hardware Reference</i> | This guide specifies the hardware components that build a Safety Manager project. |
| The <i>Withdrawn Hardware Reference</i> | This guide specifies all withdrawn hardware components and identifies alternatives for maintaining Safety Manager projects containing withdrawn hardware. |
| The <i>Software Reference</i> | This guide specifies the software functions that build a Safety Manager project and contains guidelines on how to operate them. |
| The <i>On-line Modification Guide</i> | This guide describes the theory, steps and tasks related to upgrading Safety Builder and embedded software and modifying an application online in a redundant Safety Manager. |

Task-oriented guides

A task-oriented guide provides both procedural and basic knowledge. A task can inform the reader on *how to* perform the task in terms of steps to follow.

Additionally a task can describe *what* important considerations to make or what options to choose from when performing a task.

A task-oriented guide lists the required skills and knowledge that people must master to qualify for the described tasks.

It is common for task oriented guides to refer to reference guides for details.

Reference guides

A reference guide provides detailed information or solutions regarding its scope. A reference guide is a Safety Manager related guide and provides background information to support tasks as described in task-oriented guides.

A reference guide does not describe tasks in terms of *how to* perform the task in terms of steps to follow.

Available electronic format

All guides are accessible via the Safety Manager Knowledge Builder; an Internet Explorer based viewer with extensive search and indexing options.

The Knowledge Builder contains guides stored as:



- web pages
- Adobe PDF guides

The information stored on the Safety Manager Knowledge Builder CD-ROM can be installed as stand-alone or merged with other Knowledge Builder booksets on a server.

Conventions

Symbols

The following symbols are used in Safety Manager documentation:

| | |
|---|---|
|  | Attention This symbol is used for information that emphasizes or supplements important points of the main text. |
|  | Tip This symbol is used for useful, but not essential, suggestions. |

**Note**

This symbol is used to emphasize or supplement important points of the main text.

**Caution**

This symbol warns of potential damage, such as corruption of the database.

**Warning**

This symbol warns of potentially hazardous situations, which, if not avoided, could result in serious injury or death.

**ESD**

This symbol warns for danger of an electro-static discharge to which equipment may be sensitive.

Fonts

The following fonts are used in Safety Manager documentation:

Emphasis

- “... inform the reader on *how to* perform the task in terms of...”
- “...see the *Overview Guide*”

Label

“The **Advanced** tab of the **Properties** window has..”

Steps

Take the following steps:

1. Create a plant and set its properties.
2.

User Variable

..create the **My Projects** folder and store the **readme.txt** file here.

..press the **Tab** key..

Next press **Enter** to..

Value

“Low is the fault reaction state for digital inputs and digital outputs.”

Variable

“The syntax is: **filename** [-s] [-p]”

<http://www.honeywellsms.com>

Emphasised text is used to:

- emphasise important words in the text,
- identify document titles.

This font is used to identify labels and titles of (popup) windows.

Labels are used for Dialog box labels, menu items, names of properties, and so on.

This font is used to identify steps.

Steps indicate the course of action that must be adhered to, to achieve a certain goal.

This font is used to:

1. identify a user variable, a filename, an object or view.
2. highlight the keys the user should press on the keyboard.

User variable is a variable, an object or a view that the reader can call-up to view or to manipulate.

This font is used to indicate a value.

Value is a variable that the reader must resolve by choosing a pre-defined state.

This font is used to identify a variable.

Variables are used in syntax and code examples.

This font is used to identify a URL, directing a reader to a website that can be referred to.

Contents

| | | |
|----------|---|-----------|
| 1 | The <i>Software Reference</i> | 1 |
| | Content of <i>Software Reference</i> | 2 |
| | Basic skills and knowledge | 4 |
| | Prerequisite skills. | 4 |
| | Training | 4 |
| | Safety standards for Process & Equipment Under Control (PUC, EUC) | 5 |
| | Safety Integrity Level (SIL) | 5 |
| | Safety layers of protection. | 6 |
| | Equipment Under Control (EUC) | 6 |
| | Process Under Control (PUC) | 7 |
| | Application design conform IEC 61131-3. | 8 |
| 2 | General | 9 |
| | Safety Builder packages | 10 |
| | Available packages | 10 |
| | Safety Builder tools | 11 |
| | File locations | 12 |
| | Type of information. | 12 |
| | Log files. | 13 |
| | Modify file locations and user settings | 13 |
| | Installing & removing Safety Builder | 15 |
| | Installing Safety Builder | 15 |
| | Removing Safety Builder | 20 |
| 3 | Basic concepts | 21 |
| | Safety Builder usage | 22 |
| | About the Plant and SM Controller databases. | 22 |
| | Application design rules | 22 |
| | Contents of a Safety Builder project | 23 |
| | Steps for configuring a Safety Builder project | 24 |
| | Controller status. | 24 |
| | Screen layout | 27 |
| | Work area. | 28 |
| | Menu bar | 28 |
| | Outlook bar | 29 |
| | Toolbar. | 30 |
| | Explorer bar | 30 |
| | Status bar | 31 |

| | |
|--|-----------|
| Interaction | 32 |
| Actions. | 32 |
| Keyboard shortcut and access keys | 32 |
| Mouse | 35 |
| Buttons. | 35 |
| Multi user environment | 36 |
| The relation between Plant and SM Controller databases. | 36 |
| Available file access levels and use. | 36 |
| Creating and accessing shared Plants for multiple users. | 38 |
| 4 Safety Builder configuration tools | 41 |
| Network Configurator | 42 |
| Starting the Network Configurator | 43 |
| Network Configurator menu | 44 |
| Toolbars | 47 |
| Component bar | 49 |
| Using Network Configurator. | 50 |
| Creating a physical network | 51 |
| Creating a logical network | 52 |
| Handling Plants | 55 |
| Handling Components. | 57 |
| Handling SM Controllers | 61 |
| Backup & restore. | 64 |
| Find Dialog | 67 |
| Printing | 68 |
| Configuring Physical View component properties | 72 |
| Configuring Logical View component properties. | 92 |
| Network Configurator component properties explained. | 105 |
| Hardware Configurator | 123 |
| Starting the Hardware Configurator | 123 |
| Hardware Configurator menu | 125 |
| Toolbars | 127 |
| Modules bar | 128 |
| Using Hardware Configurator. | 128 |
| Set Controller properties | 129 |
| Setup the cabinet assembly | 129 |
| Configuring Chassis | 130 |
| Modules and slots | 131 |
| Print | 132 |
| Find Dialog | 133 |
| Hardware component properties | 133 |
| Point Configurator. | 141 |
| Starting the Point Configurator | 142 |
| Point Configurator menu | 144 |
| Toolbars. | 146 |
| Views bar. | 147 |

| | |
|---|------------|
| Using the Point Configurator. | 147 |
| Working with Views | 148 |
| Configuring Views. | 152 |
| Working with points | 156 |
| Configuring a point | 158 |
| Importing and exporting points | 162 |
| Find Dialog | 164 |
| Print | 166 |
| Point properties | 167 |
| Application Editor. | 178 |
| Starting the Application Editor | 178 |
| Application Editor Menu | 180 |
| Toolbars | 182 |
| FLD's bar. | 183 |
| FLD layout. | 183 |
| Using the Application Editor. | 185 |
| FLD types | 187 |
| Handling FLDs | 189 |
| Adding logic symbols | 200 |
| Drawing logic | 216 |
| Creating Revisions. | 219 |
| Finding points | 220 |
| Printing | 221 |
| Application Compiler | 226 |
| Starting the Application Compiler. | 226 |
| Application Compiler menu | 229 |
| Using the Application Compiler | 229 |
| Creating a Controller file. | 230 |
| Migrating applications. | 234 |
| Starting the Migrate Application | 234 |
| Migrate Application menu. | 237 |
| 5 Safety Builder on-line tools | 239 |
| Controller Management. | 240 |
| Starting Controller Management | 241 |
| Controller Management menu. | 243 |
| Toolbars | 245 |
| Component bar | 245 |
| Using Controller Management | 245 |
| Connecting to a Controller | 246 |
| Diagnostic messages and databases. | 247 |
| Diagnostic tools. | 248 |
| Load Controller | 251 |
| Status | 253 |
| Remote Reset. | 259 |
| Time synchronization | 260 |

| | |
|---|------------|
| Application Viewer | 261 |
| Starting the Application Viewer | 262 |
| Application Viewer menu | 263 |
| Toolbars | 264 |
| FLD bar | 264 |
| Using Application Viewer | 265 |
| Viewing FLDs on-line | 265 |
| Forcing and writing points | 268 |
| 6 Miscellaneous Safety Builder tools | 271 |
| Find | 272 |
| Configuration | 274 |
| Options | 274 |
| Audit Trail | 276 |
| Event justification | 276 |
| Audit Trail Viewers | 277 |
| Event generating actions | 279 |
| Archiving events | 279 |
| Security | 281 |
| Entering password | 282 |
| Changing passwords | 283 |
| Password active period | 284 |
| Forgotten supervisor password | 284 |
| APPENDIX A Communication | 285 |
| APPENDIX B FLD symbols | 345 |
| APPENDIX C Safety Manager system points | 381 |
| APPENDIX D Point attributes | 391 |
| APPENDIX E Import and Export | 409 |
| APPENDIX F Sequence of events (SOE) | 441 |
| APPENDIX G Diagnostic information | 457 |
| APPENDIX H Configuration errors and warnings | 483 |
| List of abbreviations | 515 |
| Safety Manager Glossary | 519 |

Figures

| | | |
|-----------|---|-----|
| Figure 1 | The concept of layers of protection | 6 |
| Figure 2 | Example FLD layout | 8 |
| Figure 3 | Safety Builder settings. | 14 |
| Figure 4 | Safety Builder main screen | 27 |
| Figure 5 | Part of Safety Builder menu bar | 28 |
| Figure 6 | Keyboard access to menu items via the Alt key | 33 |
| Figure 7 | Keyboard access to dialog buttons via the keyboard. | 34 |
| Figure 8 | Examples of pop-up windows informing that you are locked-out | 37 |
| Figure 9 | Network Configurator screen | 43 |
| Figure 10 | The default Logical Network Properties window. | 55 |
| Figure 11 | Plant migration is required. | 56 |
| Figure 12 | Hovering the mouse over a component. | 61 |
| Figure 13 | Controller migration is required. | 62 |
| Figure 14 | The default Logical Network Properties window. | 116 |
| Figure 15 | Hardware Configurator screen | 124 |
| Figure 16 | Point Configurator main screen. | 142 |
| Figure 17 | Point Configurator Views | 149 |
| Figure 18 | The point listing ‘All points located SYS’ reordered | 151 |
| Figure 19 | Point Configurator Save As. | 151 |
| Figure 20 | Typical point properties window | 168 |
| Figure 21 | Application Editor screen | 179 |
| Figure 22 | FLD layout (hardcopy) | 183 |
| Figure 23 | Scaling FLDs. | 187 |
| Figure 24 | Equation file table | 189 |
| Figure 25 | Creating a new FLD | 190 |
| Figure 26 | Nesting FLDs | 195 |
| Figure 27 | Import FLD wizard page 1 | 197 |
| Figure 28 | Import FLD wizard page 2 | 198 |
| Figure 29 | Import FLD wizard page 3 | 200 |
| Figure 30 | Example of an equation table designed with Notepad | 212 |
| Figure 31 | Example of an equation table designed with Excel. | 213 |
| Figure 32 | Message displayed when importing a faulty designed equation table | 214 |
| Figure 33 | Update the revision ID of a single FLD | 220 |
| Figure 34 | A warning displayed when entering the Application Compiler | 227 |
| Figure 35 | Application Compiler screen. | 228 |
| Figure 36 | Example of a log file | 231 |

| | | |
|-----------|--|-----|
| Figure 37 | Plant migration is required. | 234 |
| Figure 38 | Starting the Migrate Application function. | 235 |
| Figure 39 | Migrate Application screen | 236 |
| Figure 40 | Example of the Controller Management screen | 242 |
| Figure 41 | Controller Management warning display | 242 |
| Figure 42 | Actual Diagnostics screen | 249 |
| Figure 43 | Diagnostics from Database screen | 250 |
| Figure 44 | Loop Monitoring screen | 251 |
| Figure 45 | Load Controller screen | 253 |
| Figure 46 | System Information screen | 254 |
| Figure 47 | Communication Status | 257 |
| Figure 48 | Application Viewer screen | 262 |
| Figure 49 | Example of an FLD viewed online | 266 |
| Figure 50 | Audit trail event justification window. | 276 |
| Figure 51 | Audit Trail Viewer main screen | 278 |
| Figure 52 | Physical and logical links | 287 |
| Figure 53 | Point to point link | 288 |
| Figure 54 | Example of a multidrop link | 289 |
| Figure 55 | Supported types of redundancy | 290 |
| Figure 56 | Data flow between SafeNet and redundant Control Processors | 291 |
| Figure 57 | Communication memory allocation per channel. | 294 |
| Figure 58 | Connecting the Ethernet switch to the USI-0001 communication modules and the LAN | 300 |
| Figure 59 | Connecting the Ethernet switch to the USI-0001 communication modules and the LAN | 300 |
| Figure 60 | Experion data area configuration | 301 |
| Figure 61 | Safety Manager–CEE communication via a redundant FTE network | 304 |
| Figure 62 | PCDI addressing and time-out schemes | 307 |
| Figure 63 | Connection examples with a redundant Safety Manager | 310 |
| Figure 64 | the Modbus Communication redundancy fail-over box | 310 |
| Figure 65 | Configuring Modbus addressing and time-out | 313 |
| Figure 66 | the Modbus Communication redundancy fail-over box | 315 |
| Figure 67 | Examples of a point-to-point and a multidrop architecture. | 319 |
| Figure 68 | 7 Safety Managers in a master/slave interconnection | 320 |
| Figure 69 | A typical SafeNet configuration. | 320 |
| Figure 70 | Physical and logical links | 321 |
| Figure 71 | Data flow between SafeNet and redundant Control Processors | 322 |
| Figure 72 | Setting predefined marker and register areas for SafeNet. | 323 |
| Figure 73 | Communication to a CP can be routed direct or via the other CP | 330 |
| Figure 74 | Communication failures are reported in this type of configuration | 331 |
| Figure 75 | Set GPS based date & time format and time zone via Plant Properties | 334 |
| Figure 76 | Setting the clock source ranking priority | 335 |
| Figure 77 | GPS is a constellation of 24 satellites orbiting the sky | 337 |
| Figure 78 | Available synchronization devices within an Experion environment | 342 |

| | | |
|-----------|---|-----|
| Figure 79 | Approximating an output value to an input value | 370 |
| Figure 80 | Input failure alarm marker function | 386 |
| Figure 81 | Diagnostic input health indicator | 387 |
| Figure 82 | Diagnostic input configuration window | 387 |
| Figure 83 | Safety Manager system information to DCS. | 389 |
| Figure 84 | Event definition for Point types AI and AO | 398 |
| Figure 85 | Setting communication allocations on an input point with location COM | 404 |
| Figure 86 | Example of an exported database open in Excel. | 410 |
| Figure 87 | Allocate a single point on multiple communication devices using duplicated fields | 418 |
| Figure 88 | Example of an Experion Station “SOE display” | 444 |
| Figure 89 | Tick <i>SOE collection</i> to configure the channel for SOE. | 447 |
| Figure 90 | Event definition for Point types AI and AO | 451 |
| Figure 91 | the user interface display of the QPP-0001 and the QPP-0002. | 458 |
| Figure 92 | Example of an Experion Station “diagnostics display”. | 463 |
| Figure 93 | State of input signals | 473 |
| Figure 94 | Failure model. | 527 |
| Figure 95 | Multidrop link | 532 |
| Figure 96 | Programmable electronic system (PES): structure and terminology. | 535 |
| Figure 97 | Schematic diagram of a SMOD with 4 channels | 542 |

Tables

| | | |
|----------|--|-----|
| Table 1 | Safety Builder packages | 10 |
| Table 2 | Required file access levels for functions or tools | 37 |
| Table 3 | IO bus configurations | 136 |
| Table 4 | Safety Manager point types | 156 |
| Table 5 | Fault Reaction settings for hardware IO | 173 |
| Table 6 | Fault Reaction settings for communication IO | 174 |
| Table 7 | Availability of IO symbols per type of FLD | 201 |
| Table 8 | Signal conversion | 209 |
| Table 9 | Actions that generate an Audit Trail entry | 279 |
| Table 10 | Privileges for different users in Safety Builder | 281 |
| Table 11 | Overview of peer-to-peer connections | 291 |
| Table 12 | Supported PCDI function codes | 304 |
| Table 13 | Supported PCDI error codes | 305 |
| Table 14 | Fault Reaction settings for communication IO | 306 |
| Table 15 | Supported Modbus function codes | 311 |
| Table 16 | Supported Modbus error codes | 312 |
| Table 17 | Content of real time clock reserved registers | 316 |
| Table 18 | Configuration options for the Modbus RTU protocol | 317 |
| Table 19 | Configuration options for SafeNet protocol | 328 |
| Table 20 | Configuration options for Safety Builder protocol | 331 |
| Table 21 | Update frequency of time synchronization signals | 333 |
| Table 22 | Diagnostic inputs (health status) | 348 |
| Table 23 | Example of equation function | 369 |
| Table 24 | Safety Manager system markers | 382 |
| Table 25 | Diagnostic input markers | 383 |
| Table 26 | Safety Manager system registers | 383 |
| Table 27 | Diagnostic input registers | 383 |
| Table 28 | Safety Manager alarm markers | 385 |
| Table 29 | Safety Manager alarm registers | 386 |
| Table 30 | Diagnostic inputs (health status) | 388 |
| Table 31 | Safety Manager point types | 393 |
| Table 32 | Fault Reaction settings for hardware IO | 399 |
| Table 33 | Fault Reaction settings for communication IO | 399 |
| Table 34 | Overview of available numeric types and ranges | 400 |
| Table 35 | Database field properties table explained | 411 |
| Table 36 | Database field properties | 412 |

Table 37 Valid field values when importing digital inputs. 426

Table 38 Database field interpretation for digital outputs 428

Table 39 Database field interpretation for binary inputs 430

Table 40 Database field interpretation for binary outputs 432

Table 41 Database field interpretation for analog inputs and outputs 434

Table 42 Database field interpretation for logical symbols 437

Table 43 Messages displayed by the User Interface Display of the QPP module 459

Table 44 Possible default status messages 460

Table 45 Message types 462

Table 46 Diagnostic messages sorted by Module ID 463

Table 47 Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in low demand mode of operation 538

Table 48 Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in high demand or continuous mode of operation 539

The *Software Reference*

1

The *Software Reference* is intended primarily for the people responsible for and performing tasks related to Safety Manager.

This guide describes the functions of the Safety Builder tool and contains instructions how to use these functions.

Typical readers are engineers, who need to configure Safety Manager network, configure Safety Manager hardware, and who need to create or modify the application files for Safety Manager.

It is assumed that the reader masters the required skills and knowledge as described herein.

This section contains the following information about this guide:

| Topic | See |
|---|--------|
| Content of Software Reference | page 2 |
| Basic skills and knowledge | page 4 |
| Safety standards for Process & Equipment Under Control (PUC, EUC) | page 5 |
| Application design conform IEC 61131-3 | page 8 |



Note

This guide does not contain information related to other Honeywell Experion™ PKS systems and third-party controllers such as Allen-Bradley, series 9000, TDC 3000, Data Hiway, UDC, PlantScape, and so on.

For information about these systems, see the manufacturers book set.

Content of *Software Reference*

The *Software Reference* is a reference guide providing detailed information regarding the Safety Builder tool. A reference guide is a Safety Manager related guide and does not describe tasks in terms of *how to* perform the task in terms of steps to follow. A reference guide can provide input to support decisions required to achieve a certain objective.

| Guide | subjects |
|-----------------------------|--|
| <i>Software Reference</i>) | General <ul style="list-style-type: none"> • Safety Builder packages • Installing & removing Safety Builder • Security |
| | Basic concepts <ul style="list-style-type: none"> • Screen layout • Configuration • Interaction |
| | Safety Builder configuration tools <ul style="list-style-type: none"> • Network Configurator • Hardware Configurator • Point Configurator • Application Editor • Application Compiler • Migrating applications |
| | Safety Builder on-line tools <ul style="list-style-type: none"> • Controller Management • Application Viewer |
| | Miscellaneous Safety Builder tools <ul style="list-style-type: none"> • Find • Configuration • Audit Trail • Security |

References

The following guides may use this reference guide as a reference source:

| Guide | Description |
|--|---|
| <i>The Overview Guide</i> | This guide describes the general knowledge required, the basic functions of, and the tasks related to Safety Manager. |
| <i>The Safety Manual</i> | This guide describes the specifications, design guidelines, and safety aspects related to Safety Manager. |
| <i>The Planning and Design Guide</i> | This guide describes the tasks related to planning and designing a Safety Manager project. |
| <i>The Installation and Upgrade Guide</i> | This guide describes the tasks related to installing, replacing and upgrading hardware and software as part of a Safety Manager project. |
| <i>The Troubleshooting and Maintenance Guide</i> | This guide describes the tasks related to troubleshooting and maintaining Safety Manager. |
| <i>The System Administration Guide</i> | This guide describes the task related to administrating the computer systems used in a Safety Manager project. |
| <i>The On-line Modification Guide</i> | This guide describes the theory, steps and tasks related to upgrading Safety Builder and embedded software and modifying an application online in a redundant Safety Manager. |

Basic skills and knowledge

Before performing tasks related to Safety Manager you need to:

- Understand basic Safety Manager concepts as explained in the *Overview Guide* and the *Glossary*.
- Have a thorough understanding of the *Safety Manual*.
- Have had appropriate training related to Safety Manager that certifies you for your tasks (see the *Planning and Design Guide*).

Prerequisite skills

When you perform tasks related to Safety Manager, it is assumed that you have appropriate knowledge of:

- Site procedures
- The hardware and software you are working with. These may i.e. be: computers, printers, network components, Controller and Station software.
- Microsoft Windows operating systems.
- Programmable logic controllers (PLCs).
- Applicable safety standards for Process & Equipment Under Control.
- Application design conform IEC 61131-3.
- The IEC 61508 and IEC 61511 standards.

This guide assumes that you have a basic familiarity with the process(es) connected to the equipment under control and that you have a complete understanding of the hazard and risk analysis.

Training

Most of the skills mentioned above can be achieved by appropriate training. For more information, contact your Honeywell SMS representative or see:

- <http://www.automationcollege.com>.

Safety standards for Process & Equipment Under Control (PUC, EUC)

Safety Manager is the logic solver of a Safety Instrumented System (SIS) performing specific Safety Instrumented Functions (SIF) to ensure that risks are kept at predefined levels.

A SIS measures, independently from the Basic Process Control System (BPCS), a couple of relevant process signals like temperature, pressure, level in a tank or the flow through a pipe. The values of these signals are compared with the predefined safe values and, if needed, the SIS gives an alarm or takes action. *In such cases the SIS controls the safety of the process and lowers the chance of an unsafe situation.*

The logic in Safety Manager defines the response to process parameters.

In this context the following terms are explained in this section:

- Safety Integrity Level (SIL)
- Safety layers of protection
- Equipment Under Control (EUC)
- Process Under Control (PUC)

Safety Integrity Level (SIL)

The IEC 61508 standard specifies 4 levels of safety performance for safety functions. These are called safety integrity levels. Safety integrity level 1 (SIL1) is the lowest level of safety integrity, and safety integrity level 4 (SIL4) the highest level. If the level is below SIL1, the IEC 61508 and IEC 61511 do not apply.

Safety Manager can be used for processing multiple SIFs simultaneously demanding a SIL1 up to and including SIL3.

To achieve the required safety integrity level for the E/E/PE safety-related systems, an overall safety life cycle is adopted as the technical framework (as defined in IEC 61508).

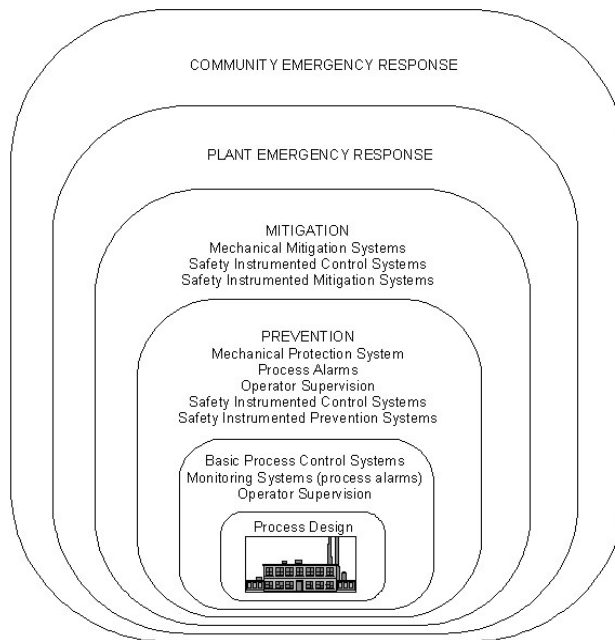
Safety layers of protection

Figure 1 on page 6 shows the typical risk reduction methods or safety protection layers used in modern process plants.

Safety Instrumented Systems (SIS) are designed to operate in the prevention and mitigation layers to:

- Prevent a process from entering a dangerous state.
- Mitigate the consequences of entering a dangerous state.

Figure 1 The concept of layers of protection



Equipment Under Control (EUC)

Safety-related systems, such as Safety Manager, are designed to prevent the EUC from entering a dangerous state and to mitigate any EUC that has gone into a dangerous state.

For these functions a safety related system can be split in:

- Emergency shutdown systems, operating in the prevention layer of Figure 1 on page 6.
- Fire and gas detection and control systems, operating in the mitigation layer of Figure 1 on page 6.

Process Under Control (PUC)

PUC is EUC expanded with regulations to prevent the process from running out of control or to mitigate the consequences when it does run out of control.

Where PUC is concerned, Safety Manager monitors the process for abnormal situations. Safety Manager is able to initiate safety actions and process alarms.

Such actions and alarms can be caused by abnormal situations in the:

- Process
- Safety loops
- Safety system itself.

Application design conform IEC 61131-3

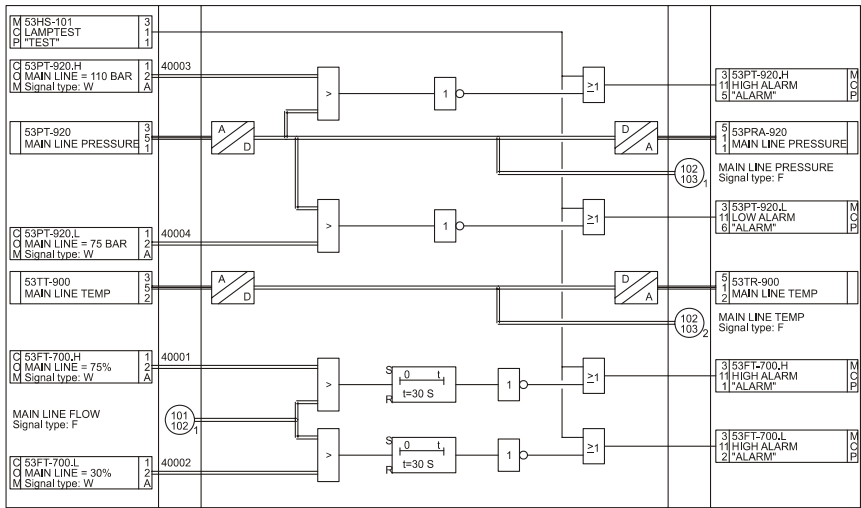
The IEC 61131 standard defines, as a minimum set, the basic programming elements, syntactic and semantic rules for the most commonly used programming languages, including graphical languages of:

- Ladder Diagram,
- Functional Block Diagram and,
- Textual languages of Instruction List and structured Text;

For more information see the IEC web site.

Figure 2 on page 8 shows how Safety Manager uses the graphical programming method, based on Functional Block Diagram as defined by the IEC 61131-3.

Figure 2 Example FLD layout



General

2

This section describes general Safety Builder information.

| Topic | See |
|--------------------------------------|---------|
| Safety Builder packages | page 10 |
| File locations | page 12 |
| Installing & removing Safety Builder | page 15 |

Safety Builder packages

Available packages

The Safety Builder software is available in a variety of packages.

A unique license number is issued to each customer. This number, together with the standard installation package, determine the installation and operation of the appropriate software package.

The available Safety Builder software packages are:

- **Demo.** This package has limited functionality and serves primarily for demonstration purposes. You cannot print nor create/view a logical view.
- **Contractor.** This package has limited functionality and allows Safety Manager contractors to design a system.
Contractors use Safety Builder in the pre-engineering phase only.
- **Basic.** This package offers all Safety Builder functions.

Table 1 on page 10 lists the features of the various software packages.

Table 1 Safety Builder packages

| Tools | Safety Builder packages | | |
|------------------------|-------------------------|------------|-------|
| | Demo [*] | Contractor | Basic |
| Network Configurator | Yes | Yes | Yes |
| Hardware Configurator | Yes | Yes | Yes |
| Point Configurator | Yes | Yes | Yes |
| Application Editor | Yes | Yes | Yes |
| Application Compiler | | | Yes |
| Controller Management | | | Yes |
| Application Viewer | | | Yes |
| Import and Export | | | Yes |
| Migrating applications | | | Yes |
| Audit Trail | Yes | Yes | Yes |

^{*} Max. one plant, one Controller and 10 sheets

Safety Builder tools

Safety Builder has two main functionalities:

- Offline: software engineering tool for Safety Manager.
- On-line: user interface to Safety Manager.

For this, Safety Builder offers an extensive range of tools. Note that some of these tools may not be available, depending on your license and package.

| Configuration tools | |
|-----------------------|--|
| Network Configurator | Here, you define where Safety Manager is located in the available networks. |
| Hardware Configurator | In this tool, you define the type and location of the cabinet, chassis and modules for Safety Manager. |
| Point Configurator | Here, you set all the properties of the points in the current system. |
| Application Editor | With this tool, you can design the Functional Logic Diagrams. |
| Application Compiler | Enables you to verify the syntax, completeness and consistency of the configuration. You can also compile the configuration to a controller file which can be uploaded to the SM Controller. |

| On-line tools | |
|-----------------------|---|
| Controller Management | Enables you to load and retrieve controller files and view the diagnostics and system status. |
| Application Viewer | In this Viewer, you can monitor values within FLDs while the application is running. |

In addition a third set of tools is available:

| Miscellaneous tools | |
|---------------------|--|
| Find | This tool helps to find items in a project. The dialog boxes are optimized for the type of item you are looking for. |
| Configuration | This tool allows you to change user settings. |
| Audit Trail | This tool allows you to access the logging of all functional changes to the application. |
| Security | With this tool you control access to tools, functions and plants by means of password protection. |

File locations



Caution:

Safety Builder performs many built-in checks to guarantee the integrity of the data.

Unauthorized handling of this data, such as manual file modification, renaming files or folders, etc. may result in corruption or a permanent loss of data.

Type of information

When installing Safety Builder, the following data is installed by default:

1. Program files

A folder is created to store the Safety Builder program files.

By default this folder is created under the **program files** folder of Windows. No application related data is stored in this folder.

This folder and its content are removed when uninstalling Safety Builder.

2. Project information

A folder is created to store project information. The default folder name is **safetybuilder** but may be renamed.

This folder does not necessary have to be located on the same media as the program files: It is advised to relocate this folder to a network server when you want to access the Plant with multiple configuration engineers simultaneously (see “Multi user environment” on page 36 for details).

The project information folder contains all application related files and other project related data. The user is free to create or assign other (sub)folders to store project and /or Controller information.

The project information contained herein is *not* removed when uninstalling Safety Builder.

3. General information

General information, such as the location of project files, is stored in a dedicated folder under **Documents and Settings\All users** or **Documents and Settings\Current USER**, depending on the installation settings made in “Customer Information” on page 17.

This information is *not* removed when uninstalling Safety Builder; A new instance of Safety Builder will locate and use this information to i.e. locate the project information.

4. **USER settings**

USER settings, such as preferences, last opened, etc. are stored in the **Current USER** folder, created by Windows under the **Documents and Settings** folder.

The information stored herein will i.e. determine how and on what location Safety Builder will start or continue when you run it.

Log files



Tip:

Archiving your Audit Trail events on a regular basis will improve Safety Builder performance. For details see “Archiving events” on page 279.

The following log files are stored and accessible by the user:

- **Compilation log**
For instructions on how to access, see “Compilation log file” on page 230.
- **Audit Trail log**
For instructions on how to access, see “Audit Trail” on page 276.
- **Diagnostic log**
For instructions on how to access, see “Diagnostic tools” on page 248.
- **Migration log**
For instructions how to access, see “Migration log file” on page 237.

Modify file locations and user settings

File locations

In order to modify file locations it is recommended to:

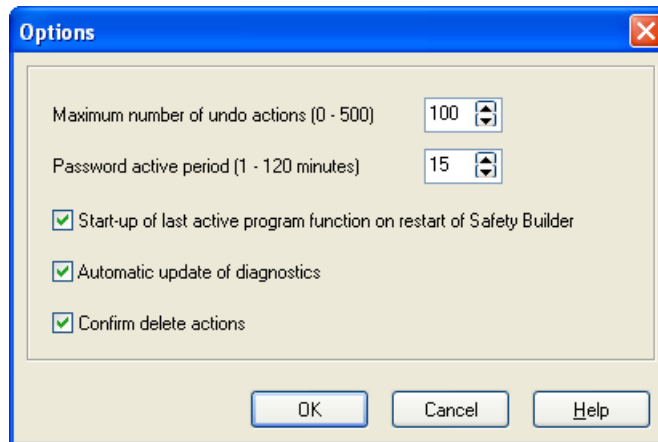
- uninstall and re-install Safety Builder with new file locations, or
- assign new file locations using the “Plant properties” on page 72 and “Physical SM Controller properties” on page 75 or
- backup and restore your Plant to a new location. For details see “Backup & restore” on page 64.

Safety Builder settings

You can modify Safety Builder settings as indicated in Figure 3 on page 14.

For usage information about this window see “Options” on page 274.

Figure 3 Safety Builder settings



Installing & removing Safety Builder

This section gives information about the installation and removal of Safety Builder. Actual information about the installation procedure can be found in the “Release letter” bundled with Safety Builder.

The installation program installs the software functions activated by the unique license number that the customer has purchased from Honeywell. Before you can start the application, you must verify whether you have the appropriate license number.

Installing Safety Builder

Safety Builder is usually supplied on CD ROM. Every standard Safety Builder license allows you to install the software onto a maximum of five computers.

The described installation procedure assumes you use the English version of Windows 2000 or XP and that you choose English as the Setup language. You need administrator rights in Windows 2000/XP to be able to install the Safety Builder software.

Necessities



Note:

When installing Safety Builder it may be required that you restart your station.

Before you install Safety Builder make sure you have the following:

- official Honeywell Safety Builder installation CD ROM,
- serial code,
- license number.

Also make sure the computer you are installing on, has the following requirements:

Minimum requirements for Safety Station

Basically any modern PC can qualify as a Safety Station.



Caution

1. These requirements only apply to a Safety Station. They may be insufficient for an Experion[™] Station.
 2. The current Knowledge Builder engine that provides access to the user guides, does not run on Windows 2000: When running Windows 2000 you can request and install an older version of the Knowledge Builder engine, install Knowledge Builder on another machine or extract the PDF version of the user guides from the Knowledge Builder CD ROM. For more information contact Honeywell SMS.
-

The minimum requirements for a Safety Station are:

- Windows XP SP1 or Windows 2000 SP4,
- Pentium 1Ghz, 256 MB RAM, 20 GB free disk space, CD ROM,
- screen resolution 1024×768, 16-bit color.

As most Experion Stations have higher requirements, most Experion Stations can be upgraded to a Safety Station.

Optimal performance requirements for Safety Station

The following requirements are additional to the minimum requirements:

- screen resolution 1280×1024, 16-bit color,
- 100 Mbps NIC,
- RS485 interface.

Previous installations of Safety Builder software

Setup checks whether another version of the Safety Builder software has been installed on your PC. If it detects one, Setup asks you whether you would like to remove the “old” software or it will install the “new” software in an alternative folder.

Installation procedure

To install Safety Builder follow the following steps:

- 1 Close all Windows applications that are open.
- 2 Put the Safety Builder distribution CD ROM in the CD ROM drive.
- 3 The installation program starts automatically. If it does not, start SETUP.EXE located in the root folder of the CD ROM.
- 4 A welcome screen of the Setup program appears. Click **Next** to start the Setup program for the Safety Builder software.

- 5 Walk through the below described steps, following the instruction on-screen
 - a. License Agreement,
 - b. Customer Information,
 - c. License Number,
 - d. License Number,
 - e. Select Program Folder,
 - f. Default Home Page,
 - g. Components,
 - h. Overview,
 - i. Setup Completed.

License Agreement

The first step in installing the software, is accepting the license agreement. Carefully read the license agreement before proceeding. You must accept the license agreement before you can continue. To accept the license agreement and continue with the installation, click the **Yes** button. If you decline the license agreement, click the **No** button; the setup procedure will be aborted.

Customer Information

Enter the user name and the company name. In the **serial Number** text box, enter the serial number supplied with the distribution CD ROM. Please note that letters in the serial number are case-sensitive ('x' is not the same as 'X'). You must enter a valid serial number before you can install Safety Builder. After you have successfully filled the **USER Information** dialog box, click the **Next** button.

At the **Install this application for:** option, choose **Anyone who uses this computer (all users)** or **Only for me (<username>)** depending on who you want to give access to Safety Builder.

License Number

A dialog box appears, prompting you to enter the license number supplied with the distribution CD ROM. This number determines which Safety Builder package you are entitled to use. Setup automatically installs the correct package. Please note that letters in the serial number are case-sensitive ('x' is not the same as 'X'). You must enter a valid license number before you can proceed. After you enter a valid license number, click the **Next** button.

Choose Destination Location

You are prompted to indicate the hard disk directory the Safety Builder application files must be installed in. The default destination folder is X:\program files\Honeywell SMS\SM Safety Builder\R131, where 'X' is the drive that

contains the Windows 2000/XP operating system (usually drive C:). Either accept this default suggestion or click use the **Browse** button to specify a different folder. When you are done, click the **Next** button.

Please note the following considerations:

- The installation folder must be called 'Safety Manager';
- Long file names are supported;
- Folder and file names (without extension) shorter than nine characters may only contain one dot.

Select Program Folder

In this screen you can choose the location where the program icons will be put. You can accept the default location or select a custom location.

Default Home Page

You can choose to make the Honeywell web site your home page.

Components

Safety Builder makes use of some 3rd party software. This software is provided in the Safety Builder installation CD ROM and can automatically be installed during installation of Safety Builder.

The main 3rd party components that are automatically installed and/or updated are:

- MS Direct Access Components (MDAC)
- MS XML parser

Overview

The following screen displays an overview of the Safety Builder components that will be installed. Click the **Next** button which starts the actual installation.

Wait while the installation takes place. When the installation is completed you are prompted with the **Setup completed** dialog.

Setup Completed



Attention:

If you use Safety Manager as part of Experion you must hereafter perform the installation steps in “Update diagnostic messages in Experion server” on page 19.

This dialog informs you that set up has been completed. Click **Finish** to exit the set up program. You are now ready to use Safety Builder.

Update diagnostic messages in Experion server

If you use Safety Manager as part of Experion™ you must also update the diagnostic files on Experion servers prior to R300.

Take the following steps:

- 1 Browse to the `Experion message files` folder on the Safety Builder distribution CD ROM.
- 2 Select and copy the following files:
 - `fsc_module.txt`
 - `fsc_fault.txt`
- 3 Locate the same files on the Experion server.
These files are usually stored in `\Experion PKS\server\Data`.
- 4 Paste the files from the Safety Builder distribution CD ROM.
Herewith you overwrite the same files in the Experion server.

Removing Safety Builder



Note:

Files and registry entries created after Safety Builder was installed, will not be removed. This means the project files in the project sub folders will not be deleted from your hard disk. If you want to remove them, you need to delete them manually.

To remove Safety Builder:

1. In the **Control Panel**, double-click **Add/Remove Programs** (program components may have different names in non-English Windows versions).
2. From the list of applications that can be automatically removed by Windows 2000/XP, select **Honeywell SMS SM Safety Builder** and click the **Change/Remove** button.
3. A window will appear, asking you to **Modify and repair** or **Remove all** the software. Choose **Remove all** and click **Next** to remove the Safety Builder.
4. Confirm the uninstall by clicking **OK** in the pop-up window.
 - This will *not* uninstall your application files.

Basic concepts

3

This section describes the general Safety Builder layout.

It describes the basic software properties and explains how the layout can be configured. It also clarifies the different interaction methods used in the software.

This section covers the following topics:

| Topic | See |
|------------------------|---------|
| Safety Builder usage | page 22 |
| Screen layout | page 27 |
| Interaction | page 32 |
| Multi user environment | page 36 |

Safety Builder usage

Safety Builder is the configuration, maintenance and on-line tool for Safety Manager. Its functions are listed in “Safety Builder tools” on page 11.

Safety Builder is therefore the main software tool on every Safety Station.

About the Plant and SM Controller databases



Note:

The Plant and SM Controller databases overlap in several areas: Changing properties or values in the Plant database can affect the properties and values in an SM Controller database and vice versa.

Safety Builder stores all configuration settings and application data entered for the Plant and the SM Controllers in dedicated databases.

The main differences between a Plant and a SM Controller database are:

- The Plant database stores all communication related settings and the main configuration settings of an SM Controller.
You can modify a Plant database via several Safety Builder tools. The most important tool is the Network Configurator.
A Plant database has the extension `.CAC`.
- The SM Controller database stores all remaining controller related configuration settings and contains all application related data, such as point data and functional logical diagrams (FLDs).
You can modify an SM Controller database via several Safety Builder tools. The main tools to modify an SM Controller database are: Hardware Configurator, Point Configurator and Application Editor.
An SM Controller database has the extension `.CC`.

Application design rules

Application design rules are basic sequencing rules of “programming order” that must be adhered while configuring a project using Safety Builder.

If the application design rules are not adhered correctly, the prerequisites for a function requested may not be fulfilled. In such cases Safety Builder shows the function or tool shaded (dimmed) until the prerequisites are fulfilled.

In short, application design rules are straight forward rules that:

1. Demand that conditions to use a function or tool have been fulfilled prior to actually using the function or tool.
2. Prompts a user when deleting components that contains underlying components. If the user chooses to continue, Safety Builder de-allocates or deletes any underlying components.

Example

- Before allocating a point to an IO module, an IO module of the correct type must have been allocated in an IO chassis.
 - To allocate an IO module, an IO chassis must be allocated first.
 - In order to allocate the IO chassis, a Controller must be created and the type and allocation of the IO chassis herein must be defined.
 - To create a Controller, a Plant and a network structure must be defined first.
-

Example



Tip:

1. Safety Builder warns the user, before actually deleting or de-allocating underlying components.
 2. Accidental deletions or de-allocations can be undone with the undo function.
-

- When deleting an IO module from an IO chassis, all points allocated to that module will be de-allocated.
 - When deleting an IO chassis, all IO modules of that IO chassis will be deleted, and all points assigned to the deleted IO modules will be de-allocated.
-

Contents of a Safety Builder project

A Safety Builder project consists of:

- Configurations for one or more Safety Manager systems consisting of:
 - Hardware
 - Points
 - Functional Logic Diagrams
- Communication configuration of the Safety Manager systems to communicate with i.e.:
 - Safety Station, other Safety Managers

- Experion™ PKS server, CEE controllers, Modbus devices
- System software and compiled application files, once translated.
- Diagnostic files, once loaded from the running SM Controller.

Steps for configuring a Safety Builder project

Configuring Safety Manager with Safety Builder is typically done by taking the following steps:

- 1 Use the Network Configurator to define a physical and logical network for Safety Manager.
For more information, see “Network Configurator” on page 42.
- 2 Use the Hardware Configurator to define what hardware (cabinets, chassis, modules) is used and where it is allocated in Safety Manager.
For more information, see “Hardware Configurator” on page 123.
- 3 Use the Point Configurator to define and allocate points to Safety Manager.
For more information, see “Point Configurator” on page 141.
- 4 Use the Application Editor to make Functional Logic Diagrams for Safety Manager.
For more information, see “Application Editor” on page 178.
- 5 Use the Application Compiler to make a controller file that can be loaded into Safety Manager.
For more information, see “Application Compiler” on page 226.

Controller status



Tip:

The steps to change the Controller status are described in “Set Controller loaded” on page 64.

The status of an SM Controller is indicated by the color and boldness of its description text in the Explorer bar and in the Work area (see “Screen layout” on page 27 for locations).

- The colors used indicate the status of the SM Controller, see “SM Controller text color” on page 25.
- A bold text indicates a selected SM Controller, see “Selected SM Controller” on page 25.

SM Controller text color

The status of the SM Controller is indicated by means of colored text:

- When *black* is used to display a SM Controller name, the SM Controller has been properly configured and loaded into the system. (See also “Set Controller loaded” on page 64.)
- When *red* is used to display a SM Controller name:
 - the configuration of the SM Controller is not completed and loaded into the system or
 - the configuration of the loaded SM Controller changed since it was loaded and needs to be reloaded, or restored as described in “Backup & restore” on page 64.

Selected SM Controller



Tip:

A selected SM Controller is displayed bold, all other SM Controllers are displayed in normal font.

You can only select one SM Controller at a time. All actions you perform will be related to the selected SM Controller.

If you want to select a SM Controller see “Selecting an SM Controller” on page 61.

About properties and settings



Note:

Always backup before you access a project.

Safety Builder uses data-aware components to display and change project properties and settings. Data-aware components derive and store their values directly from and to disk.

The moment you make changes to project properties and /or settings you thereby change certain project files stored on disk. This means that the original project gets overwritten and is “lost”, the moment you make a change to an application setting.



Notes:

1. *Changing a value back to its original state does not undo that change*; it just makes another change.
 2. Undo can only undo one action: If your change started a chain of actions you might not be able to use undo to recover from that change.
-

To overcome accidental loss of data you must make a backup before you browse/change a project. For more about creating (and restoring) a backup see “Backup & restore” on page 64.

Screen layout

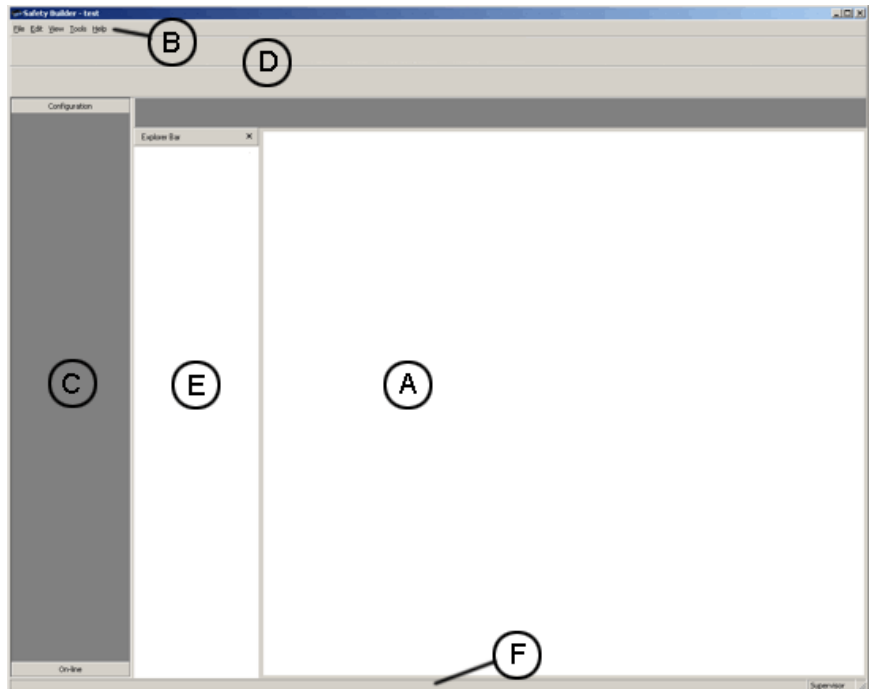
When you launch Safety Builder, the main screen appears, which resembles Figure 4 on page 27.



Notes:

- Depending on the configuration, Safety Builder can also launch the last used program function on startup. (See “Options” on page 274).
- To activate possible hidden bars click **View** and select the bar you want to display.

Figure 4 Safety Builder main screen



- A Work area
- B Menu bar
- C Outlook bar

- D Toolbar
- E Explorer bar
- F Status bar

Work area

This part of the interface contains the active tool.

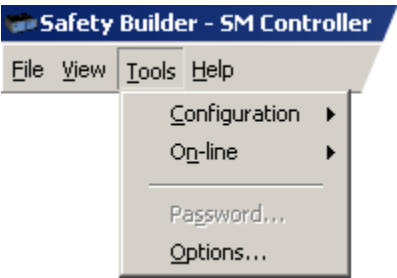
When looking at Figure 4 on page 27 you see the work area without any tool being active. If no tool is active the work area is empty.

Menu bar

The Safety Builder menu bar functions in a similar way to menu bars in other Windows programs.

General menu items, such as *Tools* in Figure 5 on page 28, are always visible. Program specific items are only visible when the corresponding program is active. These items differ per program.

Figure 5 Part of Safety Builder menu bar



The access keys, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also “Keyboard shortcut and access keys” on page 32.

The menu bar contains at least the following items:

| | |
|------------------------------|-------------------------------------|
| <i>File</i> | |
| <hr/> | |
| > C lose | Closes the active program function. |
| > E xit | Exits Safety Builder. |
| <i>View</i> | |
| <hr/> | |
| > T oolbars | Toggles display of the toolbars |
| > O utlook Bar | Toggles display of the outlook bar |
| > A udit trail Viewer | Launches the Audit Trail Viewer |

Tools

| | |
|-------------------------|--|
| > C onfiguration | Displays a sub menu with available configuration tools. The following tools are available: <ul style="list-style-type: none"> • Network Configurator • Hardware Configurator • Point Configurator • Application Editor • Application Compiler |
| > O n-line | Displays a sub menu with available on-line tools. The following tools are available: <ul style="list-style-type: none"> • Controller Management • Application Viewer |
| > P assword | Launches the Security tool. |
| > O ptions | Enables you to set general program options. |

Help

| | |
|-------------------------------|---|
| > S afety Builder help | Launches the Safety Builder Help function. |
| > A bout | Shows current version and license of the program. |

Depending on the active program function, the menu bar is expanded with tool-specific items. For more information select a tool menu section from the sections discussing:

- “Safety Builder configuration tools” on page 41.
- “Safety Builder on-line tools” on page 239.

Outlook bar

The Outlook bar is part of the application shell rather than a program function. It shows the different program functions, so you can quickly switch from one program function to another.

The outlook bar consists of two panels: **Configuration** and **On-line**. These can be accessed by clicking the corresponding buttons at the top or bottom of the bar.

- The configuration section displays the following: Network Configurator, Hardware Configurator, Point Configurator, Application Editor, Application Compiler.
- The on-line section displays the following: Controller Management, Application Viewer.

Show/hide the Outlook bar

Hiding the Outlook bar will increase the active work area.

With the Outlook bar hidden, click **Tools>Configuration** or **Tools>On-line** from the Menu bar to select the desired program function.

- To hide the Outlook bar, click the **X** in the top right corner of the Outlook bar.
- To toggle between show and hide, click **View>Outlook Bar** from the Menu bar.

Toolbar



Note:

A toolbar only shows the most used tool functions and components. Some tool functions and components have to be accessed via an item in the Menu bar.

A toolbar contains a subset of tools or components that can be used by the active program.

Multiple toolbars can be active at the same time.

Show/hide the Toolbar

Hiding a Toolbar will increase the active work area.

If the Toolbar is hidden you can still select items from the toolbar: Click an item from the Menu bar to select a desired tool button.

To toggle between show and hide, click **View>Toolbars** from the Menu bar and toggle the toolbar on or off.

Explorer bar

This section of the interface is tool-specific; its function differs per tool. The explorer bar functionality for each tool is described in subsections of “Safety Builder configuration tools” on page 41.

Show/hide the Explorer bar

Hiding an Explorer bar will increase the active work area.

If the Explorer bar is hidden you must click **View>Explorer bar** from the Menu bar to unhide the Explorer bar.

- To hide the Explorer bar, click the **X** in the top right corner of the Toolbar.
- To toggle between show and hide, click **View>Explorer Bar** from the Menu bar.

“Controller status” on page 24 explains how you should interpret the various colors of the SM Controllers listed in the Explorer bar.

Status bar

Shows current status information about the Safety Builder.


The status bar consists of two parts:

- The left part shows tool specific actual program information.
- The right part shows the current security status. For more information see “Security” on page 281.

The on-line program function also show the fault status, date, time, operating temperature, status of the force enable key switch and the number of active forces of Safety Manager.

Interaction

This section gives a general description of the concepts of interaction with Safety Builder. You can use both keyboard and mouse for interaction with Safety Builder.



Note:

To reduce user errors, Safety Builder only shows permissible operations. This means certain program features can be disabled occasionally.

Actions

Most of the components in Safety Builder support the following basic actions, similar to other software:

| | |
|--------|--|
| Cut | Delete the current selection and add it to the copy buffer. |
| Copy | Copy the value of current selection into the copy buffer. |
| Paste | Paste the value of the copy buffer at the currently selected location. |
| Delete | Remove the current selection. |
| Undo | Reverses the last action. |
| Redo | Redo the last undo action. |

Keyboard shortcut and access keys

Shortcut and access keys are designed to speed up user activity by navigating through Safety Builder via the keyboard.

Safety Builder has shortcut and access keys for:

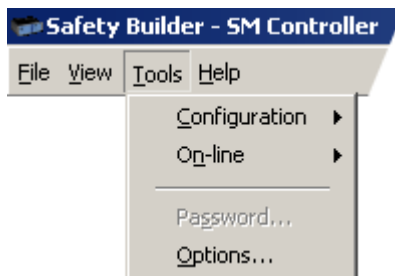
- Menu items, as described in “Menu bar” on page 28
- Toolbar items, as described in “Toolbar” on page 30
- Explorer bar buttons, as described in “Explorer bar” on page 30
- Pop-up menu items, with the main buttons described in “Buttons” on page 35.

Tool menu access keys

Tool menus often contain one underscored character per menu item, called access keys. Access keys can be activated by pressing the **Alt** key.

Figure 6 on page 33 indicates that you can press and release **Alt**, then **T**, and then **O** to call-up the **Tools>Options** window. In these *User Guides*, the access key is indicated by a bold face type, such as the “**O**” in “**Options**”.

Figure 6 Keyboard access to menu items via the **Alt** key



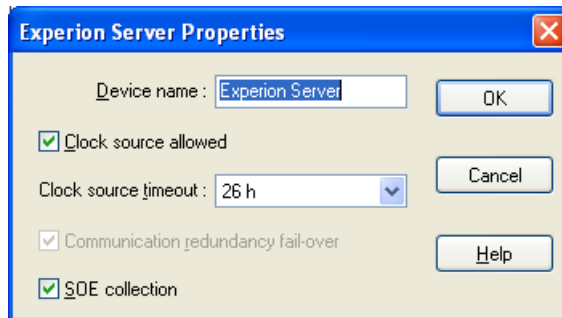
To view the tool specific access keys, see the sections describing the tool menus:

- “Network Configurator menu” on page 44,
- “Hardware Configurator menu” on page 125
- “Point Configurator menu” on page 144
- “Application Editor Menu” on page 180
- “Application Compiler menu” on page 229
- “Controller Management menu” on page 243
- “Application Viewer menu” on page 263

Dialog boxes

- Dialog boxes, as shown in Figure 7 on page 34 often contain one underscored access key per menu item, tab or button. These can be activated by:
 - a. typing the underscored access key of an item name (e.g press **D** to change the *Device name*.)
 - b. pressing the **Tab** key until the desired item is selected. Next press **Enter** to activate the item.

Figure 7 Keyboard access to dialog buttons via the keyboard



Global shortcut keys



Note:

If shortcuts contain a plus sign, for example **Ctrl+P**, you need to press -and hold down- **Ctrl** and then press **P** to open a **Print** dialog.

Below a listing is provided of global shortcut keys, which you can use in most components of the software:

| | |
|---------------|------------|
| Ctrl+A | Select All |
| Ctrl+C | Copy |
| Ctrl+F | Find |
| Ctrl+P | Print |
| Ctrl+V | Paste |
| Ctrl+X | Cut |
| Ctrl+Z | Undo |
| Del | Delete |
| F1 | Help |

To view the tool specific access keys, see the sections describing the tool menus:

- “Network Configurator shortcut keys” on page 51,
- “Hardware Configurator shortcut keys” on page 128
- “Point Configurator shortcut keys” on page 148
- “Application Editor shortcut keys” on page 186

- “Application Compiler shortcut keys” on page 230
- “Controller Management shortcut keys” on page 246
- “Application Viewer shortcut keys” on page 265

Mouse



Note:

On most computers the primary mouse button is the left button, and the secondary button is the right button. But some computers are configured with these buttons switched.

In line with most other Windows programs, Safety Builder works best with a mouse. Although most tasks can be accomplished with only a keyboard, using a mouse will make most tasks easier.

There are several basic mouse actions used in Safety Builder:

| | |
|--------------|--|
| Click/Select | Positioning the pointer over an object and then pressing and releasing the primary mouse button. |
| Double-click | Positioning the pointer over an object and then pressing and releasing the primary mouse button twice in rapid succession. |
| Drag | Positioning the pointer over an object, then pressing the primary mouse button down and holding it while moving the mouse. |
| Context menu | On most sections of the screen you can use the secondary mouse button to activate the context menu. This menu shows context sensitive functions that can be used here. |

Buttons

On many screens the following generic buttons appear:

| | |
|--------|--|
| OK | Press the OK button to store and apply the user configurable properties and options and to return to the previous screen. |
| CANCEL | Press the CANCEL button to reject the changes that are made to the user configurable properties and options and to return to the previous screen. |
| APPLY | Press the APPLY button to store and apply the user configurable properties and options. |
| HELP | Press the HELP button to open help on the active window. |

Multi user environment

If the application folders are stored on a shared location (i.e. a network drive) you can access a Plant and its SM Controllers with up to five users simultaneously.

This section informs you about the accessibility and locking policies that Safety Builder enforces when accessing a Plant with multiple users at the same time.

The relation between Plant and SM Controller databases



Notes:

Safety Builder may deny you access to Plant and/or SM Controller database in order to:

1. Allow access to multiple users simultaneously: This requires the Plant and/or SM Controller databases to be shared, so *exclusive access is denied*.
2. Warrant the integrity of Plant and SM Controller databases: This forces Safety Builder to only allow exclusive access to a database. Hence, *shared access is denied*.

The Plant and SM Controller databases overlap in several areas: Changing properties or values in the Plant database can affect the properties and values in an SM Controller database and vice versa.

Therefore changes can only be done when exclusive file access is granted.

For more information see “About the Plant and SM Controller databases” on page 22.

Available file access levels and use



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
2. To give up exclusive access to an SM Controller access the **Network Configurator**.
3. To give up shared access exit the tool or function that demands shared access.

To give up all access you close the tool or task (click **File>Close** from the menu bar) or you exit Safety Builder.

Locks on the Plant and SM Controllers control user access to the Plant and SM Controller databases.

Figure 8 on page 37 shows examples of pop-up windows you might get if the required access level is locked by another user.

When you are locked-out you cannot continue until the indicated user frees the lock.

Figure 8 Examples of pop-up windows informing that you are locked-out

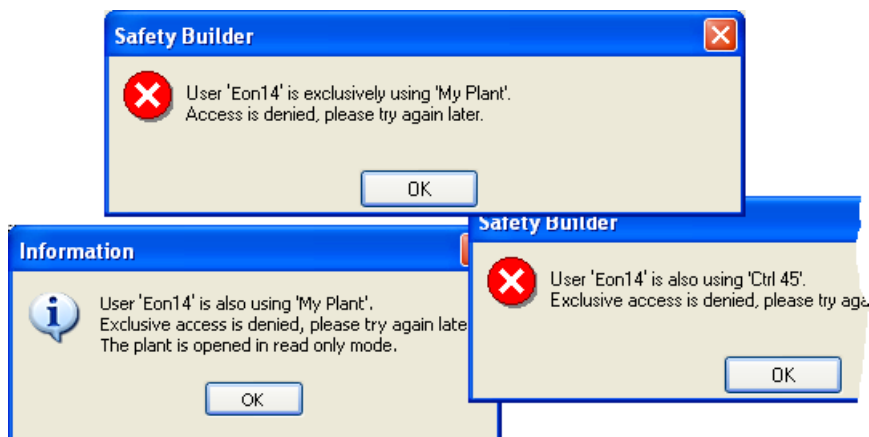


Table 2 on page 37 shows which access level is required for what tasks, i.e. what locks are applied when executing a task.

For more information on access levels see:

- “Exclusive access” on page 38
- “Shared access” on page 38
- “Read-only access” on page 38

Table 2 Required file access levels for functions or tools

| Desired access to function or tool | Required access level to the database: | |
|---|--|--------------------|
| | <Plant> .CAC | <SM Controller>.CC |
| Select SM Controller (Network Configurator) | read only access or higher | not applicable |
| Start Plant Configuration (Network Configurator) | exclusive access | not applicable |
| Application Migration Tool | exclusive access | exclusive access |
| Hardware Configurator | shared access | exclusive access |
| Point Configurator* | shared access | exclusive access |
| Application Editor | shared access | exclusive access |
| Application Compiler | shared access | exclusive access |
| Controller Management | shared access | shared access |

Table 2 Required file access levels for functions or tools (*continued*)

| Desired access to function or tool | Required access level to the database: | |
|---------------------------------------|--|--------------------|
| | <Plant> .CAC | <SM Controller>.CC |
| • Load SM Controller | shared access | exclusive access |
| Application Viewer | shared access | shared access |

- * - Modifying SafeNet points requires exclusive access to impacted SM Controllers.
- Import requires exclusive access to Plant and all SM Controller databases.

Exclusive access

You need exclusive access to a Plant and/or SM Controller database when changing properties or data stored in that database (see Table 2 on page 37).

- Exclusive access to a database is *denied* when exclusive or shared access has already been granted to another user.

Shared access

You need shared access to a Plant and/or SM Controller database when performing actions that require the database but will not conflict with similar actions performed by other users at the same time (see Table 2 on page 37).

- Shared access to a database is *denied* when exclusive access has already been granted to another user.

Read-only access

Read-only access applies to **Network Configurator** only.

This allows you to achieve read-only access to a locked Plant database in order to select an SM Controller for use in another tool or function.

Creating and accessing shared Plants for multiple users

A Plant and the components it contains must be placed in a shared network environment to be accessible to multiple users.

In principle any Plant can be made accessible to multiple users.

Creating a shared Plant

To share a Plant for multiple users you must locate the Plant folder on an accessible (shared) network location, when creating the Plant as described in “Creating a new Plant” on page 55.

Other users can now establish access to this shared Plant. To do this see “Accessing a shared Plant” on page 39.

Accessing a shared Plant



Tip:

Safety Builder will remember the location of this Plant; you only need to do this once.

To create access to a shared Plant:

- 1 In **Network Configurator** drag a **Plant** icon from the **Button Bar**
- 2 Access the **Plant properties** and click the “...” button
- 3 Navigate to the shared network location and open the <Plantname> .CAC file. (see “Plant properties” on page 72 for details).

Safety Builder configuration tools

4

This section describes the various configuration tools available in the different Safety Builder packages.

These tools are used to configure and build the Safety Manager application files.

For an overview of the tools available for each package, see “Safety Builder packages” on page 10.

| Tool | See |
|------------------------|----------|
| Network Configurator | page 42 |
| Hardware Configurator | page 123 |
| Point Configurator | page 141 |
| Application Editor | page 178 |
| Application Compiler | page 226 |
| Migrating applications | page 234 |

Network Configurator

The Network Configurator tool in Safety Builder enables you to configure the network layout of your safety system. It also lets you select a Controller, which you then can configure.

The Network Configurator is used to do the following:

- Create a clear physical network overview.
- Create a logical network.
- Define the network properties for all the components used in the network.

For more information on designing a safety network, see the *Planning and Design Guide*.

This section covers the following topics:

| Topic | See |
|--|---------|
| Starting the Network Configurator | page 43 |
| Network Configurator menu | page 44 |
| Toolbars | page 47 |
| Component bar | page 49 |
| Using Network Configurator | page 50 |
| Creating a physical network | page 51 |
| Creating a logical network | page 52 |
| Handling Plants | page 55 |
| Handling Components | page 57 |
| Handling SM Controllers | page 61 |
| Backup & restore | page 64 |
| Find Dialog | page 67 |
| Printing | page 68 |
| Configuring Physical View component properties | page 72 |
| Configuring Logical View component properties | page 92 |

Starting the Network Configurator

To activate Network Configurator, you either:

- Click the corresponding icon in the **Outlook bar**
- Click **Tools > Configuration > Network Configurator** from the **Menu bar**
- Press the shortcut keys **Alt, T, C, N**

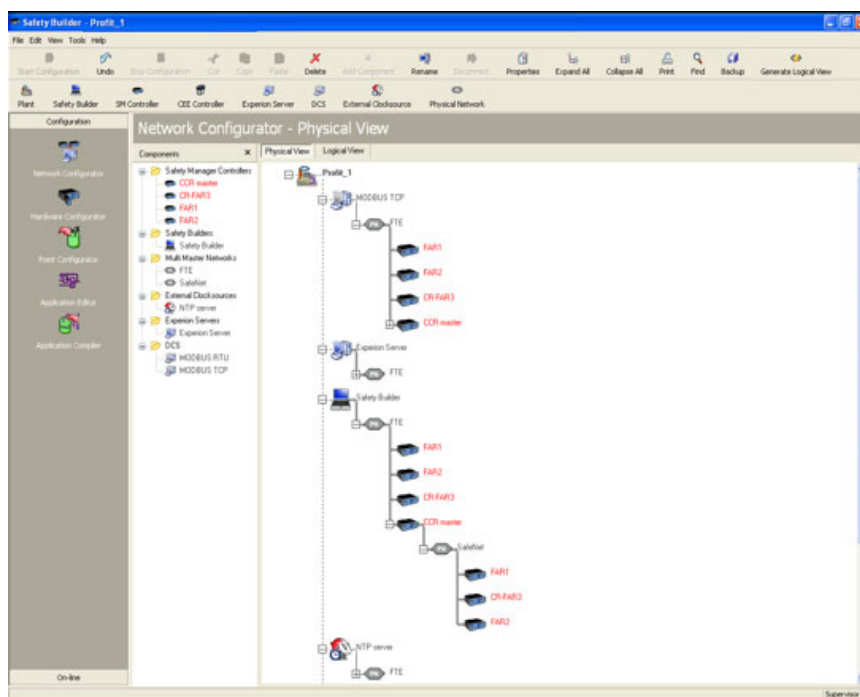


Note:

If you get a popup stating exclusive access is denied see “Working in a multi user environment” on page 44.

The **Network Configurator** screen appears, which resembles Figure 9 on page 43.

Figure 9 Network Configurator screen




This program window consists of the following sections:

- The menu bar, toolbars, outlook bar and status bar.
For a description of these bars see “Screen layout” on page 27.

- The explorer bar in Network Configurator is referred to as Component bar. It contains a list of all components in the current network. The selected component is highlighted.
- The work area, which displays either a physical view or a logical view of the current network, identified by the **Physical View** tab and the **Logical View** tab (for more information see “Physical & Logical Views” on page 50).

Working in a multi user environment



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
2. To give up shared access exit the tool or function that demands shared access.

To give up all access you can close the file (click **File>Close** from the menu bar).

When you try to access the Plant database with multiple users simultaneously, access to this tool may be limited or denied:

- If the Plant database is opened for shared use exclusive access to Network Configurator is denied and you get a popup stating:
Exclusive access is denied, please try again later.
- If the Plant database is opened exclusive use by some one else, access is denied and you get a popup stating:
Access is denied, please try again later.

In above cases, you cannot continue until the “denied access” lock is relieved by the other user(s).

For more information see also “Multi user environment” on page 36.

Network Configurator menu

Below list shows the Safety Builder Network Configurator menu structure.

The shortcut access key combinations, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also “Keyboard shortcut and access keys” on page 32.

| Menu item | Description |
|-------------------------------|---------------------------------------|
| File | |
| > C lose | Closes the Network Configurator. |
| > S tart Configuration | Start configuring the selected plant. |
| > S top Configuration | Stop configuring the selected plant. |

| | |
|--------------------------------|---|
| > <i>Change Password</i> | Change a password (see “Changing passwords” on page 283). |
| > <i>Print</i> | Activates the print dialog (see “Printing” on page 68). |
| > <i>Backup</i> | Back up the current configuration (see “Backup Plant” on page 65). |
| > <i>Restore Configuration</i> | Restore a configuration (see “Restore Plant” on page 66). |
| > <i>Generate Logical View</i> | Automatically generate a Logical View from the Physical View (see “Physical & Logical Views” on page 50). |
| > <i>Exit</i> | Exits Safety Builder. |

| Edit | |
|--------------------------------|---|
| >Undo | Undo the last action. Safety Builder supports multiple undo's. |
| >Cut | Delete the current selection and add it to the copy buffer. |
| >Copy | Copy the value of current selection into the copy buffer. |
| >Paste | Paste the value of the copy buffer at the currently selected location. |
| >Delete | Delete the current selection (see “Deleting components” on page 58). |
| >Add Component | Add the active component to the selected component. |
| >Rename | Change the name of the selected component. |
| >Disconnect | Disconnect the relation between the component and its “parent”. |
| >Properties | View or edit the properties of the selected component |
| >Find | Opens up the find dialog (see “Find Dialog” on page 67). |
| >Select Controller | Select a controller for further configuration. |
| >Enable "Disconnected" Load | Enables or disables manually setting the load status. |
| >Set Controller Loaded | Set the status of the controller to Loaded . |
| >None | Deselects items in the components bar. |
| >Plant | Select Plant in the components bar. |
| >Safety Builder | Selects Safety Builder in the components bar. |
| >SM Controller | Selects SM Controller in the components bar. |
| >CEE Controller | Selects Experion™ CEE controller in the components bar. |
| >Experion server | Selects Experion™ server in the components bar. |
| >DCS | Selects DCS or Modbus device in the components bar. |
| >External Clocksource | Selects an PTP or NTP based External Clock source in the components bar. |
| >Physical network | Selects a Physical network in the components bar. |
| >Add Logical Connection | Creates a new logical connection in the logical connection table. (Only available in Logical View .) |

View

| | |
|-----------------------------------|---|
| > T oolbars | Toggles display of the toolbars. |
| > O utlook Bar | Toggles display of the Outlook bar. |
| > A udit trail Viewer | Launches the Audit Trail Viewer (see “Audit Trail” on page 276). |
| > C omponents | Toggles display of the Components bar. |
| > P hysical View | Switches to Physical View (see “Physical & Logical Views” on page 50). |
| > L ogical View | Switches to Logical View (see “Physical & Logical Views” on page 50). |
| > E xpand all | Expand the entire network view (see “Collapsing and expanding nodes” on page 56). |
| > C ollapse all | Collapse the entire network view (see “Collapsing and expanding nodes” on page 56). |
| > C ompilation Log File | Opens the Application Compiler log file. |

Tools

| | |
|-------------------------|---|
| > C onfiguration | Displays a sub menu with available configuration tools. For an overview see “Safety Builder configuration tools” on page 41. |
| > O n-line | Displays a sub menu with available on-line tools. |
| > P assword | Launches the Security tool (see “Entering password” on page 282). |
| > O ptions | Enables you to set general program options (see “Options” on page 274). |

Help

| | |
|-------------------------------|---|
| > S afety Builder help | Launches the Safety Builder Help function. |
| > A bout | Shows current version and license of the program. |

Toolbars

**Note:**

A toolbar only shows the most used tool functions and components. Some tool functions and components have to be accessed via an item in the Menu bar.

A toolbar contains a subset of tools or components that can be used by the active program.

Multiple toolbars can be active at the same time.

Network Configurator Operations

The Network Configurator Operations toolbar contains the most common functions of Network Configurator.

Click **View>toolbars>Network Configurator Operations** to toggle the Network Configurator Operations toolbar.

Network Configurator Components

The Network Configurator Components toolbar contains the components used for defining networks.

You can drag and drop components from the toolbar into the work area.

Click **View>toolbars>Network Configurator Components** to toggle the Network Configurator Components toolbar.

The following components are available:

Plant



The top-level of a network hierarchy.

Note that a Plant is actually a container component, containing all Safety Manager related networking configurations in a plant.

Every Safety Manager project consists of one plant.

Safety Builder



Use this component to add a Safety Station (dedicated computer running Safety Builder).

You can connect up to 4 Safety Stations per physical network.

Note that Safety Manager will not make a distinction between multiple Safety Stations on one physical link - all are seen as one.

SM Controller



Use the SM Controller to define the network locations of the controllers in your safety system.

You can connect up to 63 SM Controllers in a network.

An SM Controller can only be used in one plant.

CEE Controller



Use this component to add an CEE controller to your network configuration.

You can connect up to 8 CEE controllers per Ethernet network.

Experion server

Use this component to add an Experion™ server to your network configuration.

You can connect one Experion Server per Ethernet network.

DCS

Use this component to add a Modbus RTU or a Modbus TCP communication device to your network.

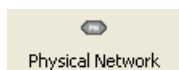
You can connect:

- one Modbus RTU master per serial network.
- up to 8 Modbus TCP masters per Ethernet network.

External Clock Source

Use this component to define an external clock source based on the PTP or NTP protocol.

You can connect one external clock source per Ethernet network.

Physical Network

Use this component to define a physical connection between SM Controllers and other network components.

Linked to an SM Controller serial communication channel you can:

- connect up to 63 SM Controllers in a SafeNet network or
- connect one network master, not being an SM Controller

Linked to an SM Controller Ethernet channel you can:

- connect up to 63 SM Controllers in a SafeNet network or
- connect up to 8 (different) Ethernet devices, not being an SM Controller

*This component is only available in the **Physical View**.*

Component bar

The Component bar is an Explorer bar that contains a list of all components in the current network. A selected component is highlighted in the Component bar.

For general information on Explorer bars see “Explorer bar” on page 30.

Use the Component bar to:

- Select and drag an existing components into the work area.
- Select a Controller to be processed by other Safety Builder tools that you access.

To select a Controller either double click the Controller or right click the Controller and click **Select Controller**.

Using Network Configurator

Use Network Configurator to:

- create and select a Plant you wish to access (see “Handling Plants” on page 55)
- select a Safety Manager you wish to access (see “Handling SM Controllers” on page 61) or
- create a network involving Safety Managers (see “Create a network” on page 51).

Plants and Components

Safety Managers, Stations and networking systems are called *Components*.

The links between these components are defined in network hierarchies. These network hierarchies are stored in a virtual component, called a *Plant*.



Attention:

If links have to be placed between components, these components must all be available in one Plant.

For examples of components see “Network Configurator Components” on page 48.

Physical & Logical Views



Note:

To define or view plant configurations you must have the plant open for configuration. You can only have one plant open for configuration at a given time. For details as how to open or close a plant for configuration see “Handling Plants” on page 55.

Network Configurator provides options to define and create a physical and a logical network between components in a plant.

Such networks can be built and viewed using the Physical and Logical View of the Network Configurator:

- **Physical View**

The Physical View represents the physical network structure.

In this View, you define which network components are used and how these components are connected physically.

For configuration details, see “Creating a physical network” on page 51.

- **Logical View**

The Logical View represents the logical structure of the network.

In this View, you define:

- a. Which network components exchange information with each other.
Two components can only exchange information if they are connected physically (directly or indirectly).
- b. The network capacity that will be reserved to exchange points between logically connected components.

For configuration details, see “Creating a logical network” on page 52.

Create a network

To create a network do the following:

- 1 Create a physical network, as explained in “Creating a physical network” on page 51.
- 2 Define the logical connections, as explained in “Creating a logical network” on page 52.

Network Configurator shortcut keys

Besides the shortcut keys listed in “Keyboard shortcut and access keys” on page 32, the following shortcut keys are activate when you use the Network Configurator:

- **F2** opens the rename function of the active component.
- **F4** opens the properties of the active component.
- **Ctrl+D** disconnects the link.
- **Ctrl+O** starts the configuration of the selected plant.
- **Ctrl+F4** stops the configuration of the selected plant.
- **Ctrl+Enter** adds the active component.
- **Ctrl+RightArrow** expands the network view.
- **Ctrl+LeftArrow** collapses the network view.

Creating a physical network

Physical networks represent the physical network structure and are created in the **Physical View**.

To switch to the Physical View, select **View > Physical View** or click the **Physical View** tab in the work area.

In the Physical View you define which network components are used and how these components are physically connected.

To create a physical network:

- 1 Define and add a plant to the work area, as described in “Adding components” on page 57. The plant acts as a container of your network.
- 2 Start the configuration of that plant, as described in “Starting and stopping a Plant configuration” on page 56.
- 3 Add components to the network as described in “Adding components” on page 57.

Properties for physical connections

Each time you add or modify a component you are prompted with its properties. To manually display the properties you must press the **F4** key when the component is selected.

For details regarding physical component properties refer to “Configuring Physical View component properties” on page 72.

Creating a logical network



Notes:

- You can build *one* logical connection between two devices that share a protocol and a (direct or indirect) physical connection.
 - An SM Controller can simultaneously support several logical connections per physical communication channel.
 - The **Logical Network Properties** window shows the properties related to the selected logical connection.
-

A logical network is a configuration of all possible peer-to-peer connections between the various components connected via the physical network (see “Creating a physical network” on page 51).

A logical network is created in the **Logical View** which basically consists of a grid with all configured logical network connection (peer-to-peer) properties.

To switch to the Logical View, select **View > Logical View** or click the **Logical View** tab in the work area.

In the **Logical View** you define:

- which two network components will be communicating with each other and
- the associated properties (such as time-out, addressing, etc.).

Create automatically



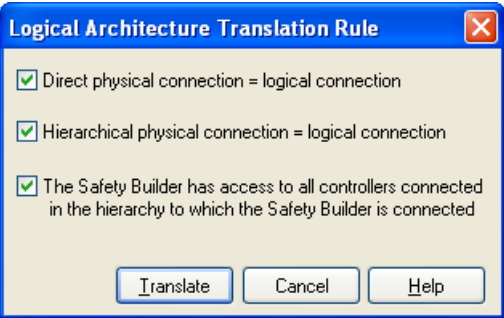
Note:

You can use the **Generate Logical View** command only when no logical connections are made.

To process modifications to an existing logical network in a later stage see “Create automatically” on page 53 and “Properties for logical connections” on page 54.

If a logical structure of the network is not yet defined, you can automatically let Safety Builder generate a Logical View from the Physical View. To do so, select **File > Generate Logical View** in the menu bar or press the **Generate Logical View** button in the button bar.

The following window appears:



- | | |
|---|--|
| Direct physical connection = logical connection | All direct physical connections are translated to logical connections. |
| Hierarchical physical connection = logical connection | All hierarchical Physical connections are converted to logical connections. |
| Safety Builder has access to all controllers connected in the hierarchy to which the Safety Builder is connected | All connections (direct and indirect) are translated to logical connections. |
| Translate | Converts Physical to Logical View with the current settings. |
| Cancel | Cancels conversion without applying changes. |

Create manually



Note:

You *cannot* build a logical connection between components if:

1. they do not have a physical connection or
2. they use a protocol that is not supported by the physical connection or
3. the communication capacity is consumed by other s.

To manually create or modify a Logical View you must do the following:

- 1 Start the configuration of the plant concerned, as described in “Starting and stopping a Plant configuration” on page 56.
- 2 Switch to the Logical View
- 3 Create a new row to add a logical connection:
 - Select **Edit > Add Logical Connection** in the menu bar or
 - press the **Add Logical Connection** button in the button bar or
 - right click in an existing row and select **Add Logical Connection** from the pop up menu.
- 4 Fill the logical connection properties:
 - a. Fill the properties directly from the grid.
With the drop down buttons that appear when you double click a cell select a master and a slave in the **Master Node** column and the **Slave Node** column and fill the remaining properties of the connection
 - b. Click the **Properties** button or press **F4** to call the **Logical Network Properties** window.

Properties for logical connections

The Logical View table has a column for each property. Depending on the type of logical connection, some property fields are omitted while others need to be filled.

To display the properties in a more fashionable order you press the **F4** key when the component is selected. This brings up the **Logical Network Properties** window as shown in Figure 10 on page 55.

For details regarding logical connection properties refer to “Configuring Logical View component properties” on page 92.

Figure 10 The default Logical Network Properties window

Handling Plants

A Plant is a basic component of every Safety Manager project containing devices, controllers as well as the physical and logical communication configurations used to interconnect these devices and controllers.

Creating a new Plant

To create a new Plant

- 1 drag a **Plant** icon from the button bar and drop it in the work area. The **Plant properties** dialog box opens.
- 2 provide the main Plant properties, such as the database folder location, as described in “Plant properties” on page 72.
- 3 click **OK** to close the **Plant properties** dialog box.

Starting and stopping a Plant configuration



Notes:

1. If you stop a Plant, you also deselect the selected SM Controller in that Plant.
2. If you start a Plant which was created with an earlier version, migration may be required.

For more about migration see “Migrating Plants” on page 56 for migration instructions.

In order to make modifications to a network you will have to **Start Configuration** of a plant. **Stop Configuration** is used to stop making modifications. When you start configuration of one plant, the configuration of all others will be stopped. This is mainly to prevent you from using one network component in more than one plants.

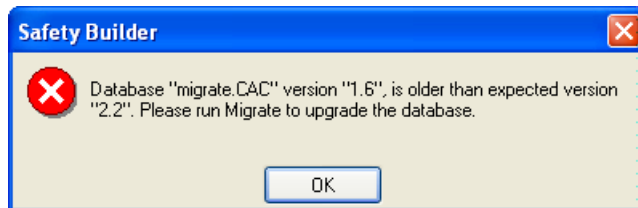
Start Configuration and **Stop Configuration** can only be chosen when a plant is selected in the work area.

Migrating Plants

When you open a Plant created with an earlier version for the first time, migration of the plant database may be required.

If required, a popup as shown in Figure 11 on page 56 will appear.

Figure 11 Plant migration is required.



For instructions as how to run Migrate Application see “Migrating applications” on page 234.

Collapsing and expanding nodes

Most network configurations contain large numbers of nodes. To keep the screen organized you can collapse all nodes and expand only to ones you want to see.

You can expand all nodes by selecting **View > Expand all** in the menu or by clicking the appropriate button in the toolbar. If you do, all nodes in the project will be displayed.

You can collapse all nodes by selecting **View > Collapse all** in the menu or by clicking the appropriate button in the toolbar. If you do, all nodes in the current project will become invisible, except the top node (plant).

You can also expand or collapse selected parts of the network configuration. You do this by double-clicking a node. All nodes below the current one are then expanded. If all nodes below the current are already expanded, then you can double-click the tree to collapse it.

Handling Components

Components are elements you can use to create network configurations.

All component types are described in “Network Configurator Components” on page 48.



Note:

More information, specific to handling SM Controllers, can be found in “Handling SM Controllers” on page 61.

Adding components

If you want to create a network in Safety Builder, you will need to add components.

To add a new component you can use one of the following methods:

- Select the component in the work area to which you want to add a new component. Then, select the component you want to add in the toolbar and click the **Add Component** button in the toolbar.
- Select the component in the toolbar, then right-click the component you want to add the component to in the work area and select **Add Component**.
- Drag the component from the toolbar to the preferred location in the work area.

In case of adding a component representing a Safety Builder, Experion™ server or Physical Network, the Network Configurator asks for the name of the new component. Type the name in the **Device name** text box and click **OK** to add the component.

In case of adding a component representing a Plant or an SM Controller, the Network Configurator asks for the name of the new component *and* a directory where to store information.

- Click on the “...” button to open a window that lets you choose a directory and a enter a name for the device.

- Type the name in the **File name** text box and click **Open** to return to the Device Properties window.
- There, click **OK** to add the component.

You can also add one components to multiple locations in the configuration. To do so, drag the relevant item from the explorer bar to the preferred location in the work area. This can for example be used when Safety Manager is connected to two different Safety Builder systems.



Note:

- The software automatically keeps track of the components that can be added to the hierarchy. This prevents placement of components at incorrect locations.
 - The first component in any Safety Builder network is always a Plant.
-

For a list of components that can be added please see “Network Configurator Components” on page 48.

Deleting components



Note:

If you delete a component that is not at the bottom of the hierarchy, all components below the deleted item will also be removed.

When a component is deleted, it is removed from the network configuration in the work area, and is removed from the Explorer bar (if it was there before the delete action).

To delete a component, select the component in the Explorer bar and then either:

- Click the **Delete** button in the toolbar.
- Right-click and select **Delete**.
- Press **Delete** on your keyboard.

Depending on your configuration a window may appear to confirm the delete action. To change this setting see “Options” on page 274.

When you have accidentally deleted a component, you can use the Undo function (in the menu select **Edit > Undo**) to restore the configuration.

Connecting components



Note:

For detailed communication configuration options see “Communication” on page 285.

All components, with exception of a Plant, can be connected to an SM Controller.

To connect to an SM Controller you must use a network component:

- To connect using a new connection:
drag the network component from the Network Configurator Components Toolbar
- To connect using a shared or existing connection:
drag the existing network component from the Explorer bar

Disconnecting components

When a component is disconnected, it is removed from the network configuration in the work area, but will remain present in the Explorer bar.

To disconnect a component, select the component in the work area and then either:

- Click the **Disconnect** button in the toolbar.
- Right-click and select **Disconnect**.



Note:

If you disconnect a component that is not at the bottom of the hierarchy, all components below the deleted item will also be disconnected.

When you’ve accidentally disconnected a component, you can use the Undo function (in the menu select **Edit > Undo**) to restore the configuration.

Moving components

Components can be moved from one place in the network to another. To do this, simply drag them (in the work area) to the desired location. Using this method you can either move a single component or move a complete network branch.

If you don’t know how to *drag*, refer to “Interaction” on page 32.

Renaming components

You can change the name of any component by selecting it and then choose **Edit > Rename** in the menu. You can only change names of components while the plant is in configuration.

Properties

Setting properties

In the Network Configurator, you can access the properties of any component.

To access component properties, either:

- Select the component and press **F4**
- Select the component and select **Edit > Properties**
- Select the component and click **Properties** in the toolbar
- Right-click the component and select **Properties**

A properties window automatically appears when you add a new component to Network Configurator.

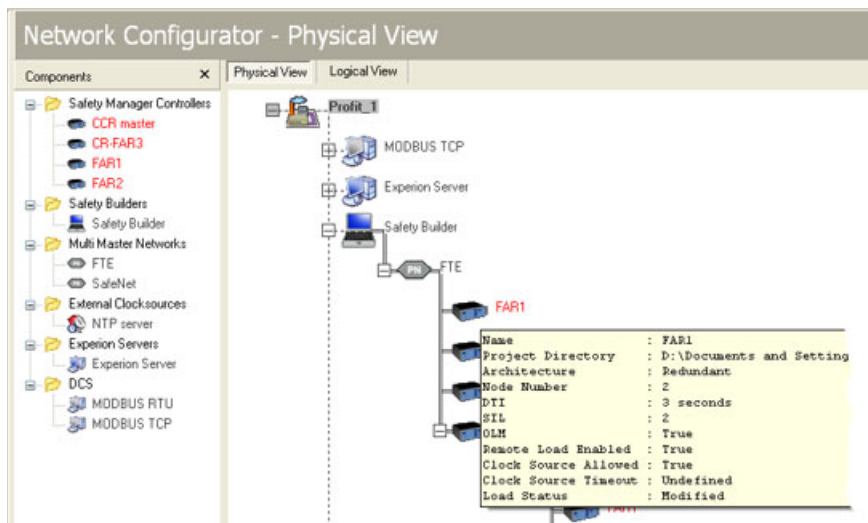
Viewing properties

Figure 12 on page 61 shows how you can quickly view the properties of a component by hovering the mouse pointer over the component. this will briefly show the properties.

After a few seconds, or when the mouse is removed, the information disappears.

A description of all properties can be found in “Physical View properties explained” on page 105.

Figure 12 Hovering the mouse over a component



Handling SM Controllers

SM Controllers are at the centre of your project. Handling SM Controllers requires special attention and provides options not available for other components.

- To handle components in general see “Handling Components” on page 57.

Selecting an SM Controller

Once you have defined your network you will have to configure the hardware of every SM Controller. To start configuring the hardware of a specific SM Controller you will need to select it in Network Configurator and then switch to the Hardware Configurator.



Note:

When opening an SM Controller created with an earlier version, migration of that controller may be required.

For more about migration see:

- “Migrating applications” on page 234 for general information,
- “Migrating Plants” on page 56 for migration instructions.

To select an SM Controller, right-click it and choose **Select controller**. The name of the selected SM Controller will be displayed in bold print.

SM Controller node number



Notes:

- Changing a node number can *not* be done on-line.
- You are allowed to assign the same node number to multiple SM Controllers within the plant, as long as these SM Controllers do not share the same SafeNet link.

The node number is a non-conflicting ID number used by SM Controllers to identify each other when communicating via SafeNet (see “Communication via the SafeNet protocol” on page 318 for more information).

When adding a new SM Controller to a plant, a non-conflicting node number (between 1 and 63) is assigned automatically.

If you like to change this number you are free to do so – but keep in mind that SM Controllers with the same node numbers cannot communicate with each other.

Migrating SM Controllers

Migration of the controller database may be required when you open a Controller which was created with an earlier version of Safety Builder.

If migration is required, a popup as shown in Figure 13 on page 62 will appear.

Figure 13 Controller migration is required.



For instructions as how to run Migrate Application see “Migrating applications” on page 234.

Copy Controller

With the copy and paste functions of Safety Builder you can copy an entire SM Controller, including point database, Controller settings and application logic and paste it *in another Plant*.

**Notes:**

The following restrictions apply when you want to copy a Controller:

1. You cannot undo when copying a Controller.
2. To copy a Controller including communication allocation, the connections and devices used for these allocations will be copied as well. If there is a (naming) conflict, copy will be aborted.
3. To copy Controllers including a shared SafeNet communication link, you should first copy the master Controller(s) followed by the slave Controller(s).

You cannot paste a copied Controller when:

- a version of that Controller already exists in the destination Plant
- the *Controller name* already exists in the destination Plant.
- a Controller *cabinet name* already exists in the destination Plant
- there is a conflict in communication configuration/allocation

To copy a Controller:

- 1 In Network Configurator select the SM Controller you want to copy.
- 2 Copy the Controller and open the Plant where you want to paste it.
- 3 To paste do one of the following:
 - a. In the Physical view click on the destination Plant node to paste the Controller in the Explorer bar of that Plant.
 - b. Open the destination Plant, select a Physical network connection and paste the Controller.
The Controller will now be pasted on to the network and a physical connection will be made. If there is a node number conflict, pasting will be aborted.

**Notes:**

1. The Controller you paste is saved in the Plant folder per default.
2. The Controller node number must be checked to match the new network architecture.
3. Communication allocations that cannot be re-established in the destination Plant will lose their communication allocation.

- 4 As soon as you paste, a dialog box is presented where you must select if you want to copy the physical and logical connections as well. When you confirm, the network connections and devices used for these connections will be copied as well. If there is a (naming) conflict, the action will be aborted.

- 5 When you successfully pasted the Controller the **SM Controller properties (physical)** window opens.
When finished copying *all* Controllers to a Plant you may want to:
 - a. define a more suitable unique Controller name for each copied Controller.
(The default assigned name is its original name.)
 - b. check and update the project file directory used to store the new Controller in.
(The default assigned project file directory is the Plant folder.)
 - c. check if the Controller node number matches the network architecture of this Plant.
Change the number if required.



Note:

When not finished copying all Controllers to a Plant you are advised to complete all copy actions for this Plant before changing names and numbers at this point. This to prevent mismatches when copying due to none matching names and node numbers.

For details about the **SM Controller properties (physical)** window see “Physical SM Controller properties” on page 75.

- 6 Press **OK** when finished.
- 7 You can now start building physical connections and logical connections as well as assigning SOE ID's and communication allocation on points.

Set Controller loaded

This function can be used to manually set the Controller status to loaded on Safety Stations that are used for engineering but not for loading.

The action to set a SM Controller loaded consists of two commands:

- **Enable “remote” load**

This option enables the command to set the Controller loaded. You should only enable the **set Controller loaded** command on engineering stations.

- **Set Controller loaded**

This option manually sets the selected Controller status to loaded. For more information regarding Controller status, see “Controller status” on page 24.

For these commands a dedicated privilege level is required. For details see “Security” on page 281.

Backup & restore

The Network Configurator is equipped with a backup and restore function.

The backup function lets you store a copy of the Plant on a disk or a network server. With the restore function, you can recover the Plant. When restoring a

Plant that was previously back upped, all modifications made since the backup will be lost.

Files included in a backup or restore

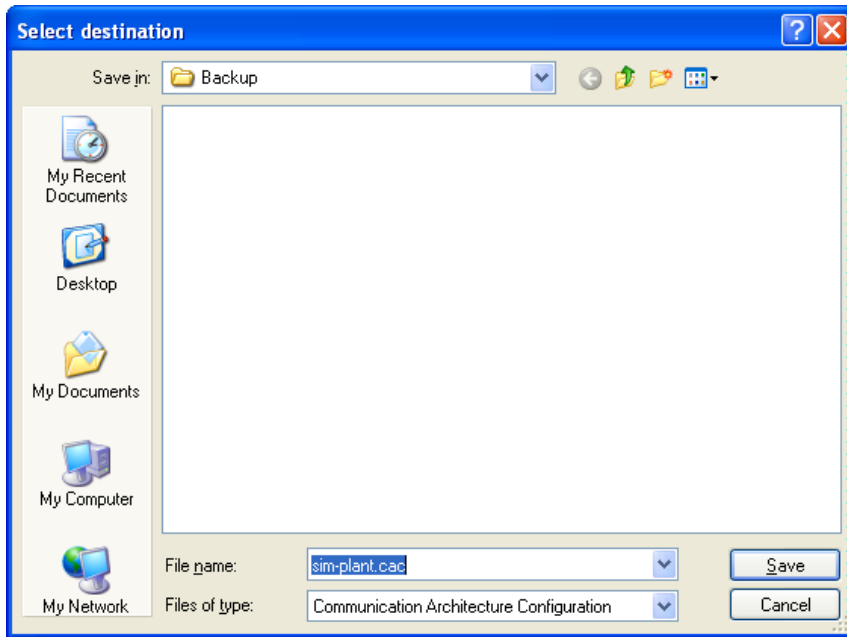
A backup is made of the following files:

- `<plant>.CAC` For the selected plant, a copy of the `<plant>.CAC` file is stored under the backup name.
The `<plant>.CAC` file contains e.g. the network configuration, a Plant wide point database and the network properties of each SM Controller.
- `<controller>.CC` For each controller in the selected plant, a copy of the `<controller>.CC` file is backed up under the original name.
The `<controller>.CC` file contains e.g. the FLDs, the SM Controller configuration and a point database.
- `<controller_file>.CCF` For each controller file of the selected plant, a copy of the `<controller_file>.CCF` file is backed up under the original name.
The `<controller>.CCF` file contains the compiled application files.
- `<controller_file>.LOG` For each controller file of the selected plant, a copy of the `<controller_file>.LOG` file is backed up under the original name.
The `<controller>.LOG` file contains the Application Compiler log files.
- `<controller_file>.DNG` For each controller file of the selected plant, a copy of the `<controller_file>.DNG` file is backed up under the original name.
The `<controller>.DNG` file is a database file containing the historical diagnostics of that controller.

Backup Plant

With the backup function, you can copy a Plant to a user-defined location. To access this function, select **File > Backup** from the menu or click the **Backup** button in the toolbar.

The following window appears:



In this window, enter a name and location of the backup file.



Warning:

It is important that you store each backup in a dedicated directory, separate from the original files.

Storing multiple plants with identical controller names in one directory results in loss of controller data.

Backup allows you to backup the <plant>.CAC file under a different name for easy reference.

You cannot rename the controller files because they are referred to by the <plant>.CAC file: *All controller files are backed up with their original name.*

Restore Plant

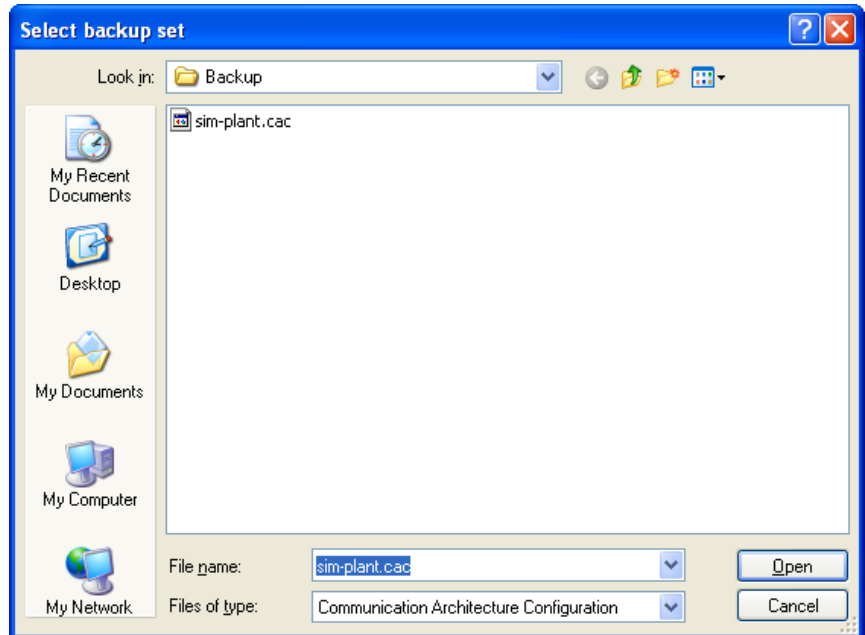
With this function you can restore a previously made backup copy.

You can access this function by

- 1 creating or selecting a new Plant (with stopped configuration)

2 selecting **File > Restore configuration** from the menu bar.

The following window appears:



In this window, select a previously back upped plant .CAC file to restore.

When you click the **Open** button a popup box appears to confirm the restore action as Restore overwrites whatever is in the selected Plant.

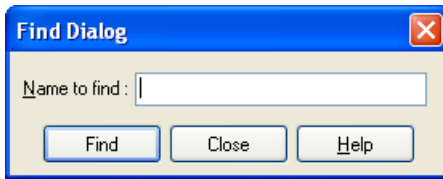


Notes:

1. Before you can restore a plant you must create a new plant using Network Configurator. The name you give to this new plant will be used when you restore a previously backed up plant.
2. You can only restore a configuration if you have previously made a backup copy (see “Backup Plant” on page 65) and the plant you want to restore to is selected and closed.

Find Dialog

In large projects you can use the find function to easily locate components. You can access this function by selecting **Edit > Find** from the menu.



Name to find

The name of the component you want to find.

- The search is case sensitive, so when you search for “test” it will not find “Test”.
- If you use the asterisk sign (*) as a wildcard, searching for “test*” will not only find “test” but also “test 1” and “test 2”.

Printing

You can print a report of the current network configuration.

To print you must open the Print Dialog. You can either:

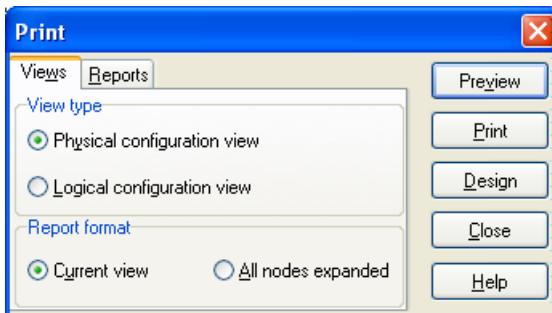
- Click the **Print** button in the toolbar
- In the menu select **File > Print**

Print Dialog

Select Report Type - Views

You can access this window by selecting **File > Print** in the menu and then selecting the **Views** tab.

This dialog lets you select the type of View you want to print.



View Type

Toggle for printing either the Physical or Logical View.

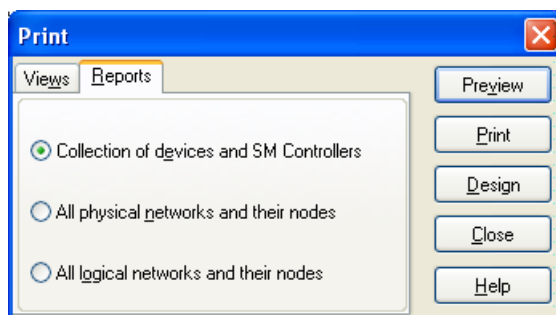
| | |
|----------------------|--|
| Report Format | Toggle for printing either the current View or to print all notes expanded. |
| Preview | Opens the preview window for the current print. |
| Print | Prints the selected configuration. |
| Design | Opens the report design utility. For more information on using this utility, see the user manual for FastReport (version 2.5). |
| Help | Launches the Safety Builder Help function. |
| Close | Close the print dialog without printing. |

Select Report Type - Reports

You can access this window by selecting **File > Print** in the menu and then selecting the **Reports** tab.

The main dialog lets you choose between:

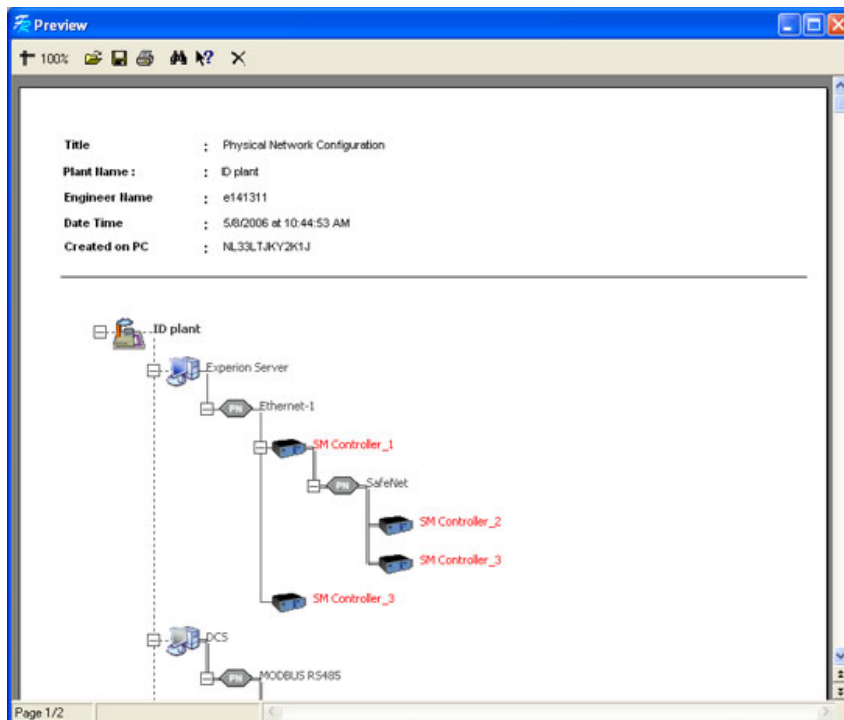
- Collection of devices and controllers
Prints an overview of the devices (Safety Builder, Experion™ server) and Safety Managers in the current configuration.
- All physical networks and their nodes
Prints a list of all physical networks and the relevant properties.
- All logical networks and their nodes
Prints an overview of all logical networks in the current configuration.



| | |
|----------------|--|
| Preview | Opens the preview window for the current print. |
| Print | Prints the selected configuration. |
| Design | Opens the report design utility. For more information on using this utility, see the user manual for FastReport (version 2.5). |
| Help | Launches the Safety Builder Help function. |
| Close | Close the print dialog without printing. |

Print Preview

Before printing to paper you can preview the output on screen. To do so select **File > Print** in the menu and press the **preview** button. The following window will then appear:



Place the mouse cursor above the buttons in the menu bar to see the texts mentioned below.

- | | |
|----------------------|---|
| Scale | Here you can adjust the zoom level to a custom value. Values can range from 15 to 250%. |
| Open report | Open a print report from file. |
| Save report | Save the print report to a file. |
| Find Text | Allows you to find a specific string in the print preview. Type the text you want to search for in the Text to find text box, define if the search should be Case sensitive and if the search should be performed on the 1st page or on the Current page . |
| Show help | Clicking on the print report after clicking on the Show help icon opens the on-line help. |
| Close preview | Close the preview window. |

Configuring Physical View component properties



Note:

Network components have both physical and logical view properties.

- the physical view properties of a component are visible in the **Physical view**
 - the logical view properties of a component are visible in the **Logical view**
-

This topic explains how you can view and edit the different physical view properties of the various Network Configurator components.

The following topics are described in this section:

- “Plant properties” on page 72
- “Safety Builder properties” on page 74
- “Physical SM Controller properties” on page 75
- “CEE Controller properties” on page 85
- “Experion server properties” on page 86
- “DCS properties” on page 87
- “External Clocksource properties” on page 88
- “Physical network properties” on page 90

Related sections:

- “Configuring Logical View component properties” on page 92
- “Network Configurator component properties explained” on page 105.

Plant properties



To access this window right-click an allocated plant and select **Properties**.

In this dialog, you can view and edit plant component properties.

Plant Name

The name of the plant. Every plant in your configuration must have a unique name.

You can enter the Plant Name directly in this text field and continue by choosing a **Database Path**, or enter the Plant Name while choosing a Database Path.

Database Path

The location where the database for the current plant is stored on disk. The Database Path can be defined by clicking on the “...” button and choosing a name and location for the plant. This field must be filled in when a new plant is created.

If you do not enter a **Plant name**, you can use this field to open an existing plant database.

Plant Wide Properties

This sections groups the plant wide properties. These properties will be enabled only when the plant is open for configuration.

Symbol Library

The symbol library sets the FLD size for the Application Editor. All available symbol libraries offer the same functionality and differ only in size and layout.

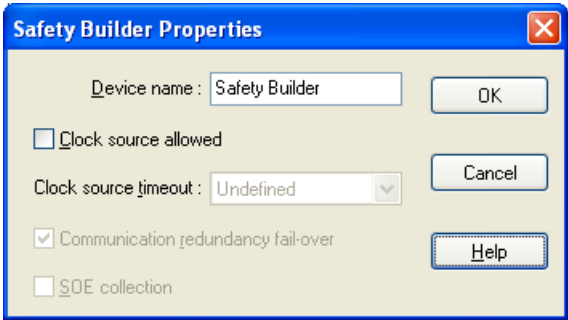
| | |
|------------------------|--|
| Degree Type | Identifies whether temperatures are to be displayed in Kelvin, degrees Fahrenheit or degrees Celsius. |
| Date Format | The format of the dates shown in Safety Builder. |
| Time Zone | Identifies the time zone applied by SM Controllers in the Plant, when synchronizing with an external clock source. |
| Honeywell (tab) | Provides access to contact information about the Honeywell organization supporting the plant. |
| Customer (tab) | Provides access to contact information about the end user of the system. |
| Plant (tab) | Provides access to contact information about the plant Safety Manager is installed in. |

Safety Builder properties



To access this window, right-click an allocated Safety Builder icon in Network Configurator and select **Properties**.

In this window, you can view and edit the physical communication properties of Safety Builders in Network Configurator.



| | |
|-----------------------------|---|
| Device name | The name of the device running Safety Builder. Every Safety Builder in your configuration must have a unique name. |
| Clock source allowed | Definition of whether or not the use of this device as clock source is allowed. Attention: Make sure that the time zone and day-light saving settings of this device match the time zone and daylight saving settings of the Plant properties . |

| | |
|---|--|
| Clock source timeout | Defines the clock source time-out period. As synchronization is a manual action, the time-out is undefined and cannot be changed. |
| Communication redundancy fail-over | Defines the fail-over response in redundant communication. As this property is fixed in the Safety Builder protocol its setting is shaded. |
| SOE collection | Not applicable for Safety Builder. |

Physical SM Controller properties



Note:

From one SM Controller you can configure up to 62 logical SafeNet connections to both master and slave SM Controllers.

To access this window, right-click an SM Controller icon in Network Configurator (Physical View), select **Properties** and select a tab.

This dialog window contains the physical communication properties of an SM Controller.

SM Controller properties (physical) - tab: General

To access this window, right-click a Safety Manager in Network Configurator (Physical View) and select **Properties**.

This tab provides access to the general properties of Safety Manager.

SM Controller Properties - SM Controller

SOE | Clock Sources | Additional Information

General | COM Module 1 | COM Module 2

Controller name : SM Controller ...

Project file directory :

Controller architecture : Redundant

Controller node number : 1

Diagnostic Test Interval : 3 seconds

Safety Integrity Level : 2

COM port : 1A

Online modification : ☒

Remote load enabled : ☐

OK Cancel Help

Controller Name

The name of the SM Controller. Every SM Controller in your configuration must have a unique name.

You can enter the Controller Name directly in this text field and continue by choosing a **Project File Directory**, or enter the Controller Name while choosing a Project File Directory.

Project File Directory

The location where the application files for the current controller are stored on the disk.

The Project File Directory can be defined by clicking on the “...” button and choosing a name and location for the SM Controller. This field must be filled in when a new controller is created.

Notes:

- To avoid overwrites and backup failures you are advised to save SM Controller files in a Plant designated folder
- If you do not enter a **Controller name**, you can use this field to open an existing SM Controller file.

| | |
|---------------------------------|---|
| Controller Architecture | <p>Definition of the SM Controller architecture being either Non-redundant or Redundant.</p> <p>Changes to this field can have implications for the availability of your project.</p> |
| Diagnostic Test Interval | <p>The Diagnostic Test Interval (measured in seconds).</p> <p>Changes to this field can have implications for the safety of your project.</p> |
| Safety Integrity Level | <p>Specification of the level of safety performance for the overall system.</p> <p>Changes to this field can have implications for the safety of your project.</p> |
| Controller Node No. | <p>Defines the node number for the Controller.</p> <p>Each Controller must have a unique node number, which can be chosen from the pull-down menu, and can have a value in the range 1 to 63. Safety Builder automatically hides node numbers allocated to other Controllers from the pull-down menu.</p> |
| COM Port | <p>Defines the COM port used to connect the SM Controller with the physical network above.</p> <p><i>Information shown here depends on the communication channel defined for the above lying physical network. It thus varies depending on the connection you identified to open the SM Controller Properties from:</i></p> <ul style="list-style-type: none"> • With 1 allocated communication module, you can choose [1A, 1B] or [1C, 1D], depending on the network protocol. • With 2 allocated communication modules, you can choose [1A, 1B, 2A, 2B] or [1C, 1D, 2C, 2D], depending on the network protocol. |
| On-line Modification | <p>Toggles of the enabling or disabling of the On-line Modification feature.</p> <p>Attention:</p> <p>Enabling the On-line Modification feature results in restricted configuration functions once you downloaded the application.</p> <p>For more information see <i>On-line Modification Guide</i>.</p> |
| Remote Load Enabled | <p>Defines if the system can be stopped, loaded and reset from a remote location.</p> <p>Note:</p> <p>You can only use this option on slave systems in a SafeNet network. Reset markers can be used to remotely reset this SM Controller. For details see “Reset markers” on page 384.</p> |

SM Controller properties (physical) - tab: COM module x



Tip:

When assigning IP addresses, gateways and subnet masks check with your organization's network administrator to identify specific addresses that may be used at your facility. While there will be no conflict with Internet networks, your organization may already use one or more of the private networks.

Below steps assist in assigning valid IP address ranges:

1. Only assign IP addresses within the IP address space reserved for private networks.
2. Follow the Experion FTE addressing guidelines when assigning IP addresses as part of an FTE network (for details see the Experion User Guides).
3. When assigning an IP address, take into account that you must assign a unique IP address for each CP.
4. *It is not allowed to use 0 or 255 at the end of an SM Controller IP address.*
5. *IP addresses of communication interface A and B of the same communication module cannot be in an overlapping subnet.*

To access this window, right-click a Safety Manager in Network Configurator (Physical View) and select a **COM module** tab.

These tabs provide access to the communication module main properties.

SM Controller Properties - SM Controller

SOE | Clock Sources | Additional Information

General | **COM Module 1** | COM Module 2

COM module type : USI_0001

COM Ports

1A FTE

| | CP1 : | CP2 : |
|-------------------|---------------|---------------|
| IP address : | 0.0.0.0 | 0.0.0.0 |
| Subnet mask : | 255.255.255.0 | 255.255.255.0 |
| Gateway address : | 0.0.0.0 | 0.0.0.0 |

1B SafeNet

| | CP1 : | CP2 : |
|-------------------|---------------|---------------|
| IP address : | 0.0.0.0 | 0.0.0.0 |
| Subnet mask : | 255.255.255.0 | 255.255.255.0 |
| Gateway address : | 0.0.0.0 | 0.0.0.0 |

1C Modbus RTU RS485

1D

OK Cancel Help

COM module type

Choose the type of communication module used for this location (the tab determines the location you look at).

The first COM module location must be occupied, the second is default set to None.

COM Ports

[1A, 1B, 1C, 1D] or
[2A, 2B, 2C, 2D]

Allows you to *view* the name of the physical connection the communication channels (ports) relate to and the type of interface used (always Ethernet based for A and B channels).

For channels A and B you can also fill the Ethernet values for **IP address**, **Subnet mask** and **Gateway address** here – values must differ for both CP1 and CP2.

For details about IP address, Subnet mask and Gateway address see the *Tip box* above.

This example shows a typical setup of channel 1A connected to the Experion™ FTE network, channel 1B used for SafeNet and channel 1C connected to a Modbus RTU device – channel 1D is unused.

To change the network assignment of a channel, open the SM Controller properties **General** tab from the position the SM Controller is attached to the Physical network connection you want to change. For details see “SM Controller properties (physical) - tab: COM module x” on page 78, section **COM Ports**.

SM Controller properties (physical) - tab: SOE



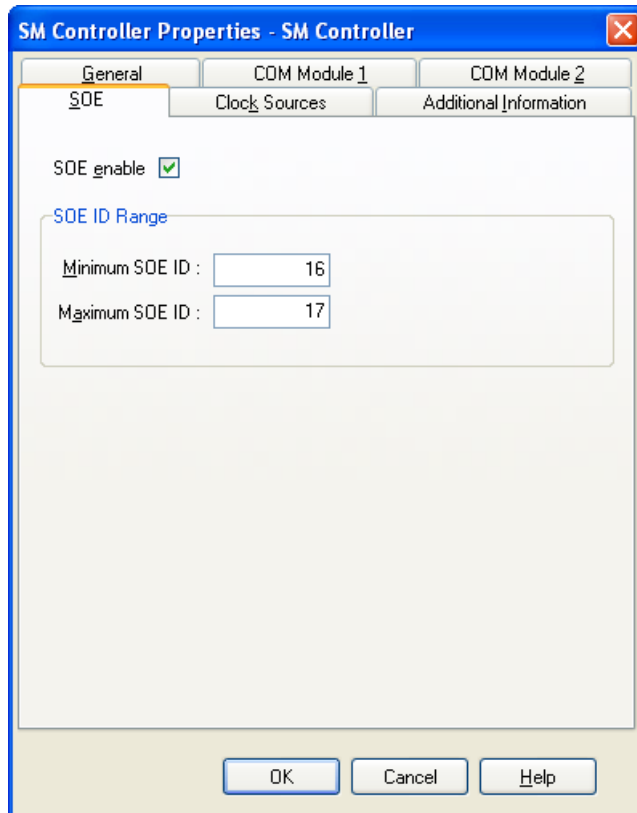
Attention:

When setting the SOE ID range:

- *make sure that the SOE ID ranges of different SM Controllers in a plant do not overlap;*
 - Safety Builder always uses 2 SOE ID's for the following system Points (*SOEBufferFull* and *ControllerFault*);
 - SOE ID's 0—15 are reserved and cannot be used.
-

To access this window, right-click a Safety Manager in Network Configurator (Physical View) and select **Properties**.

This tab provides access to the general properties of Safety Manager.



SOE enable

Enables the collection and communication of events by the SM Controller.

Note:

This box is enabled *after* you built a logical connection to a SOE collecting device.

Min SOE ID

Sets the lowest SOE ID for this SM Controller.

The **Min SOE ID** and **Max SOE ID** determine the range of SOE ID's. The smallest SOE ID range is 2.

The Min SOE ID:

- cannot be lower than 16 due to backwards compatibility with Experion™.
- should not overlap SOE ID ranges of other SM Controllers;
- must be at least 2 counts smaller than the **Max SOE ID**.

Max SOE ID

Sets the highest SOE ID for this SM Controller.

The **Min SOE ID** and **Max SOE ID** determine the range of SOE ID's. The smallest SOE ID range is 2.

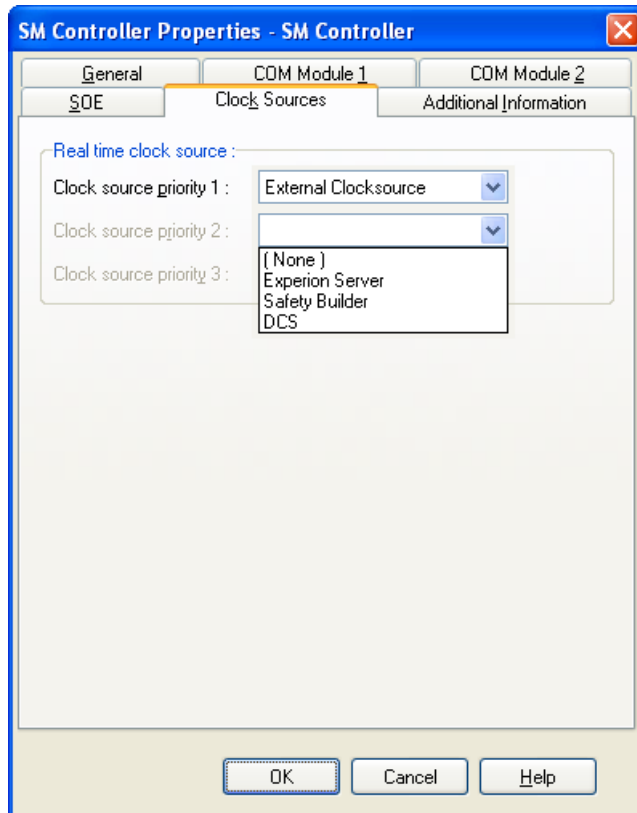
The **Max SOE ID**:

- should not overlap SOE ID ranges of other SM Controllers
- must be at least 2 counts larger than the **Min SOE ID**.

SM Controller properties (physical) - tab: Clock Source

To access this window, right-click a Safety Manager in Network Configurator (Physical View) and select **Properties**.

This tab provides access to the general properties of Safety Manager.



Real time clock source Settings of the priority level for different clock sources. By default Clock Source Priority 1 will be used. If Clock Source Priority 1 fails after the time-out, Clock Source Priority 2 will be used, etc.

Only Safety Managers and devices that are logically connected to the selected SM Controller *and* that have the option **Clock Source Allowed** checked are available in these pop-up menus:

*When all **Clock source priority x** fields are shaded this condition is not met.*

Caution:

All clock sources *must* be set to the same time zone!

SM Controller properties (physical) - tab: Additional information

To access this window, right-click one Safety Manager icon in Network Configurator (Physical View), select **Properties** and select the **Additional Information** tab.

The **Additional information** tab offers specific and descriptive details on the Controller, such as the ID, customer reference, and so on.

The screenshot shows a Windows-style dialog box titled "SM Controller Properties - SM Controller". It has three tabs: "General", "COM Module 1", and "COM Module 2". The "COM Module 1" tab is selected, and within it, the "Additional Information" sub-tab is active. The dialog contains several text input fields: "Honeywell (E) SID", "Customer reference", and "Controller description". Below these is a section titled "Principal Information" which contains fields for "Reference", "Name", "Street and number", "City", "Country", "ZIP", and "Logo" (with a browse button "..."). At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

- | | |
|-------------------------------|--|
| Honeywell (E) SID | Honeywell project identification code. The contents of this field are supplied by Honeywell. |
| Customer Reference | Identification reference of the end user. The contents of this field are supplied by Honeywell. |
| Controller Description | A short description of the SM Controller. The maximum length of the SM Controller description is 255 characters. |

Principal Information:

Reference; Name; Street
and number; City;
Country; ZIP; Logo

SM Controller specific information that will be used on the prints of your configuration.

You can use the **Logo** field to refer to an image that will be used on the prints of your configuration.

Click on the “...” button to open a window where you can open this logo.

CEE Controller properties

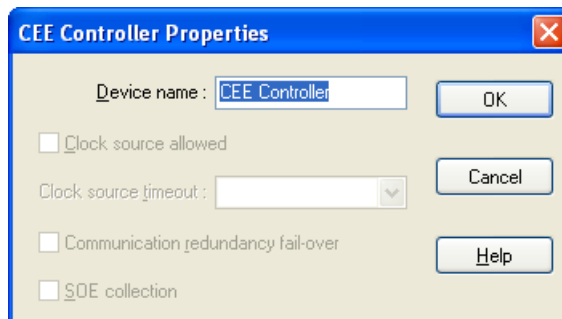


Note:

You can configure up to eight CEE Controllers per communication channel.

To access this window, right-click an allocated **CEE Controller** icon in Network Configurator and click **Properties**.

In this window, you can view and edit the physical communication properties of CEE Controllers in Network Configurator connecting via the PCDI (Peer Control Data Interface) of Experion™.



Device Name

Name of the device. Every CEE Controller in your configuration must have a unique name.

Clock Source Allowed

Not applicable for CEE Controllers.

Clock Source Timeout

Not applicable for CEE Controllers.


**Communication
redundancy fail-over**

Defines the fail-over response in redundant communication. As this property is fixed in the PCDI (Peer Control Data Interface, licensed by Experion) its setting is shaded.

SOE Collection Not applicable for CEE Controllers.

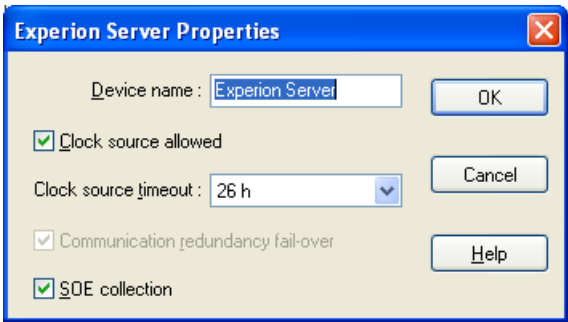
Experion server properties



 **Note:**
You can configure one Experion™ server per communication channel.

To access this window, right-click an allocated **Experion server** icon in Network Configurator and click **Properties**.

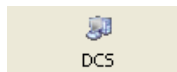
In this window, you can view and edit the physical communication properties of Experion servers in Network Configurator.



- Device Name** Name of the device. Every Experion server in your configuration must have a unique name.
- Clock Source Allowed** Definition of whether or not the use of this device as clock source is allowed.
Attention:
Make sure that the time zone and day-light saving settings of this device match the time zone and daylight saving settings of the **Plant properties**.

| | |
|---|--|
| Clock Source Timeout | <p>Defines the clock source timeout period. Values ranging from 1 min to 30 hour can be chosen.</p> <p>If no time synchronization takes place within this timeout period, an error is generated.</p> <p>Note: Experion has a default time synchronization interval of 24 hours.</p> <p>For more information about clock sources see <i>Planning and Design Guide</i>.</p> |
| Communication redundancy fail-over | <p>Defines the fail-over response in redundant communication. As this property is fixed in the Experion server protocol its setting is shaded.</p> |
| SOE Collection | <p>Assigns this device as SOE collection device.</p> |

DCS properties

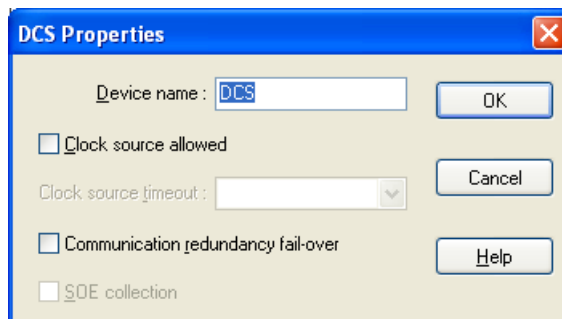


Note:

You can configure up to eight DCS (Modbus) masters per communication channel.

To access this window, right-click an allocated **DCS** icon in Network Configurator and click **Properties**.

In this window, you can view and edit the physical communication properties of the DCS component in Network Configurator.



Device Name


Name of the device.

Every DCS in your configuration must have a unique name.

| | |
|---|---|
| Clock Source Allowed | <p>Definition of whether or not the use of this device as clock source is allowed.</p> <p>Attention:</p> <ul style="list-style-type: none">• You can connect up to 8 DCS devices per channel; only one of those is allowed to act as clock source.• Make sure that the time zone and day-light saving settings of this device match the time zone and daylight saving settings of the Plant properties. |
| Clock Source Timeout | <p>Defines the clock source timeout period. Values ranging from 1 min to 30 hour can be chosen.</p> <p>If no time synchronization takes place within this timeout period, an error is generated.</p> <p>Only available when Clock Source Allowed is selected.</p> |
| Communication redundancy fail-over | <p>Defines the fail-over response in redundant communication.</p> <ul style="list-style-type: none">• check if the DCS controls the fail-over response• unchecked if SM Controller controls the fail-over response |
| SOE Collection | <p>This function is not available for DCS.</p> |

External Clocksource properties





Note:

You can configure one external clock source per Ethernet communication channel.

To access this window, right-click an allocated **External Clocksource** icon in Network Configurator and click **Properties**.

In this window, you can view and edit the physical communication properties of the external clock source configured in Network Configurator.

**Tip:**

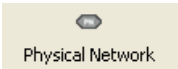
When assigning IP addresses check with your organization's network administrator to identify specific addresses that may be used at your facility. While there will be no conflict with Internet networks, your organization may already use one or more of the private networks.

Below steps assist in assigning valid IP address ranges:

1. Only assign IP addresses within the IP address space reserved for private networks.
2. Follow the Experion FTE addressing guidelines when assigning IP addresses as part of an FTE network (for details see the Experion User Guides).

| | |
|--|--|
| Device Name | Name of the device. Every external clock source in must have a unique name. |
| Clock Source Allowed | Defines that the use of this device as clock source is allowed. Note: The synchronization signals from this clock source are automatically converted to the time zone indicated in “Plant properties” on page 72. |
| Clock Source Timeout | Defines the clock source timeout period. Values ranging from 1 min to 30 hour can be chosen. If no time synchronization takes place within this time-out period, an error is generated. |
| Communication redundancy fail-over / SOE Collection | These functions are not available for external clock sources. |
| IP Address | If the External clock source is NTP based, this contains the IP address of the External Clock source. For more information on IP addressing, see separate tip. |

Physical network properties



To access this window, select a **Physical Network** icon in Network Configurator and click **Properties** from the button bar.

In this window, you can view and edit the physical network component properties.

A screenshot of the "Physical Network Properties" dialog box. It has a blue title bar with the text "Physical Network Properties" and a close button. The dialog contains several fields: "COM Port" with a dropdown menu showing "1D"; "Network Name" with a text box containing "SafeNet"; "Transport Protocol" with a dropdown menu showing "Common"; "Interface" with a dropdown menu showing "RS485"; "Baud Rate" with a dropdown menu showing "1M"; "Stop Bits" with a dropdown menu showing "1"; "Parity" with a dropdown menu showing "None"; "Signal Encoding" with a dropdown menu showing "None"; and "Network Delay (ms)" with a text box containing "0" and a spin button. At the bottom are three buttons: "OK", "Cancel", and "Help".

- COM Port

The COM port used on the master device.
- Note:

Safety Builder uses this setting to configure the COM port of the master device.

When the master device configuration is done outside Safety Builder this setting is used to log the expected configuration.
- Network Name

Name of the network.

Every network element in your configuration must have a unique name.
- Transport Protocol

Communication protocol used by this network.

This protocol changes automatically depending on the chosen setting for **Interface**.
- Interface

The interface used to connect the device to the network.

Available options: RS485, RS422, RS232 and Ethernet.

| | |
|------------------------|--|
| Baud Rate | <p>Setting of the speed of the network connection. The available options in the pull down menu differ for each interface.</p> <p>Note:</p> <p>A warning message pops-up and the communication line turns red in the network work area if the speed is set too low to transport the required network data within the available time frame.</p> |
| Stop Bits | <p>Stop bit used in communication over current network. Available options are: 1 or 2.</p> <p>This option is not available when Interface is set to Ethernet. If this option is shaded, the current value is the only one possible for the chosen network configuration.</p> |
| Parity | <p>Parity bit used for communication. Available options: None, Odd and Even.</p> <p>This option is not available when Interface is set to Ethernet. If this option is shaded, the current value is the only one possible for the chosen network configuration.</p> |
| Signal Encoding | <p>This field is only applicable for RS485 and RS422 communication. Available option is None.</p> <p>This option is not available when Interface is set to Ethernet. If this option is shaded, the current value is the only one possible for the chosen network configuration.</p> |

Configuring Logical View component properties



Note:

Network components have both physical and logical view properties.

- the physical properties of a component are visible in the **Physical view**
 - the logical properties of a component are visible in the **Logical view**
-

This topic explains how you can view and edit the different logical view properties of the various Network Configurator components.

For details on the physical view properties see “Configuring Physical View component properties” on page 72.

The following topics are described in this section:

- “About logical network properties” on page 92
- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100
- “External Clocksource Logical network properties” on page 102

Related sections:

- “Configuring Physical View component properties” on page 72.
- “Network Configurator component properties explained” on page 105.

About logical network properties

To view logical network properties you must switch to the **Logical View** of the **Network Configurator**, select a row with a logical connection and click the **Properties** button from the toolbar (or press **F4** on the keyboard). This will call-up the **Logical network Properties** window.

When determining the buffer size for markers and registers you should be aware of the address ranges, spares and communication capacity of the related physical network components.

Related topics are:

- “Communication capacity” on page 294
- “PLC address” on page 405

Safety Builder logical network properties



Notes:

- The Safety Builder marker PLC addresses range from 0 to 29999.
- The Safety Builder register PLC addresses range from 32000 to 65534.
- For a detailed description of all network properties see “Logical View property fields explained” on page 116.

A set of Safety Builder logical network properties are defined for each logical (peer to peer) connection between a Safety Station and an SM Controller.

To access this window, select or create a “*Safety Station to SM Controller*” row in the **Logical View** and click **Properties** from the tools menu.

Master Node

Contains the name of the Safety Station you want to connect.

Slave Node

Contains the name of the SM Controller you want to connect.

Protocol

Defines the Safety Builder protocol.

| | |
|---|---|
| Route | Contains the default route; change to an alternative route if desired. |
| Device address | <p>Sets the <i>Safety Station</i> (Safety Builder) device address. When replying, the SM Controller will write to this address.</p> <p>A value in the range of 1 – 63 is accepted.</p> <p>For more information see “Communication via the Safety Builder protocol” on page 329.</p> |
| Markers - In size (bytes) | <p>Defines the number of reserved bytes on the SM Controller’s communication module for the marker in buffer.</p> <p>For details see “Marker In size (bytes)” on page 118.</p> |
| Markers - Out size (bytes) | <p>Defines the number of reserved bytes on the SM Controller’s communication module for the marker out buffer.</p> <p>For details see “Marker Out size (bytes)” on page 119.</p> |
| Markers - PLC Base In | This option is used to set the base PLC addresses for input markers. For details see note above. |
| Markers - PLC Base Out | This option is used to show the calculated the base PLC addresses for output markers. For details see note above and “Marker PLC base out” on page 119. |
| Registers - In size (bytes) | <p>Defines the number of reserved bytes on the SM Controller’s communication module for the register in buffer.</p> <p>For details see “Register In size (bytes)” on page 119.</p> |
| Registers - Out size (bytes) | <p>Defines the number of reserved bytes on the SM Controller’s communication module for the register out buffer.</p> <p>For details see “Register Out size (bytes)” on page 120.</p> |
| Registers - PLC Base In | This option is used to set the base PLC addresses for input registers. For details see note above. |
| Registers - PLC Base Out | This option is used to show the calculated the base PLC addresses for output registers. For details see note above and “Register PLC base out” on page 121. |
| Enable Timeout | <p>Defines whether a time out should be used.</p> <p>When used the communication timeout can detect failure of the communication link.</p> |
| Time Out (ms) | <p>Sets the maximum communication timeout in multiples of 100 milliseconds, in case Enable Timeout is checked.</p> <p>For more information see “Timeout (ms)” on page 121</p> |
| Network delay (ms) | <p>Displays the known lag in communication.</p> <p>For more information see “Network delay (ms)” on page 122.</p> |

SafeNet logical network properties



Notes:

- The address ranges of SafeNet are not visible.
- For a detailed description of all network properties see “Logical View property fields explained” on page 116.

A set of SafeNet logical network properties are defined for each logical (peer to peer) connection between two SM Controllers.

To access this window, select or create a “*SM Controller to SM Controller*” row in the **Logical View** and click **Properties** from the tools menu.

Master Node

Contains the name of the master SM Controller you want to connect.

Slave Node

Contains the name of the slave SM Controller you want to connect.

| | |
|---|---|
| Protocol | Defines the SafeNet protocol. |
| Route | Contains the default route; change to an alternative route if desired. |
| Device address | Not used by the SafeNet protocol |
| Markers - In size (bytes) | Defines the number of reserved bytes on the communication module of the <i>master</i> SM Controller for the marker in buffer. For details see “Marker In size (bytes)” on page 118. |
| Markers - Out size (bytes) | Defines the number of reserved bytes on the communication module of the <i>master</i> SM Controller for the marker out buffer. For details see “Marker Out size (bytes)” on page 119. |
| Registers - In size (bytes) | Defines the number of reserved bytes on the communication module of the <i>master</i> SM Controller for the register in buffer. For details see “Register In size (bytes)” on page 119. |
| Registers - Out size (bytes) | Defines the number of reserved bytes on the communication module of the <i>master</i> SM Controller for the register out buffer. For details see “Register Out size (bytes)” on page 120. |
| Enable Timeout | Timeout is a means to detect failure of the communication link. For SafeNet Enable Timeout is always enabled, as an aspect to guarantee Safe communication between SM Controllers. |
| Time Out (ms) | Sets the maximum communication timeout in multiples of 100 milliseconds. For more information see “Timeout (ms)” on page 121. Note: The time out you set here contributes to the SafeNet equivalent of the DTI that can be set for a stand-alone SM Controller. |
| Network delay (ms) | Displays the known lag in communication. For more information see “Network delay (ms)” on page 122. |

CEE Controller logical network properties



Notes:

- The CEE controller marker PLC addresses range from 1 to 65535.
- The CEE controller register PLC addresses range from 1 to 65535.
Long Words and Floats get 2 PLC addresses assigned. The most significant value in the sequence is stored at the lowest storage address.
- For a detailed description of all network properties see “Logical View property fields explained” on page 116.

A set of CEE Controller logical network properties are defined for each logical (peer to peer) connection between a CEE Controller and an SM Controller via PCDI (Peer Control Data Interface).

To access this window, select or create a “*CEE Controller to SM Controller*” row in the **Logical View** and click **Properties** from the tools menu.

| | |
|-----------------------|--|
| Master Node | Contains the name of the CEE Controller you want to connect. |
| Slave Node | Contains the name of the SM Controller you want to connect. |
| Protocol | Determines that the PCDI interface will be used. |
| Route | Contains the default route; change to an alternative route if desired. |
| Device address | Set the SM Controller PCDI device address: This is the address the SM Controller will respond to. PCDI addresses between 1 – 247 are accepted. For more information see “Communication via the Peer Control Data Interface” on page 303. |

| | |
|---|--|
| Markers - In size (bytes) | Defines the number of reserved bytes on the SM Controller's communication module for the marker in buffer. For details see "Marker In size (bytes)" on page 118. |
| Markers - Out size (bytes) | Defines the number of reserved bytes on the SM Controller's communication module for the marker out buffer. For details see "Marker Out size (bytes)" on page 119. |
| Markers - PLC Base In | This option is used to set the base PLC addresses for input markers. For details see note above. |
| Markers - PLC Base Out | This option is used to show the calculated the base PLC addresses for output markers. For details see note above and "Marker PLC base out" on page 119. |
| Registers - In size (bytes) | Defines the number of reserved bytes on the SM Controller's communication module for the register in buffer. For details see "Register In size (bytes)" on page 119. |
| Registers - Out size (bytes) | Defines the number of reserved bytes on the SM Controller's communication module for the register out buffer. For details see "Register Out size (bytes)" on page 120. |
| Registers - PLC Base In | This option is used to set the base PLC addresses for input registers. For details see note above. |
| Registers - PLC Base Out | This option is used to show the calculated the base PLC addresses for output registers. For details see note above and "Register PLC base out" on page 121. |
| Enable Timeout | Defines whether a time out should be used. When used the communication timeout can detect failure of the communication link. |
| Time Out (ms) | Sets the maximum communication timeout in multiples of 100 milliseconds, in case Enable Timeout is checked. For more information see "Timeout (ms)" on page 121 |
| Network delay (ms) | Displays the known lag in communication. For more information see "Network delay (ms)" on page 122. |

Experion Logical network properties



Notes:

- Points of type DI and DO can be assigned in the range of 1 to 8192.
- Points of type AI, BI, BO and AO can be assigned in the range of 10001 to 18192.
- For a detailed description of all network properties see "Logical View property fields explained" on page 116.


A set of Experion™ logical network properties are defined for each logical (peer to peer) connection between a an Experion Server and an SM Controller.

To access this window, select or create an “*Experion Server to SM Controller*” row in the **Logical View** and click **Properties** from the tools menu.

| | |
|--------------------------|---|
| Master Node | Contains the name of the Experion Server you want to connect. |
| Slave Node | Contains the name of the SM Controller you want to connect. |
| Protocol | Defines the Experion protocol. |
| Route | Contains the default route; change to an alternative route if desired. |
| Device address | Not used. |
| Markers | Defines the number of reserved bytes on the SM Controller’s communication module for the marker in buffer. |
| - In size (bytes) | For details see “Marker In size (bytes)” on page 118. |

| | |
|---|--|
| Markers - Out size (bytes) | Defines the number of reserved bytes on the SM Controller’s communication module for the marker out buffer. For details see “Marker Out size (bytes)” on page 119. |
| Markers - PLC Base In | This option is used to set the base PLC addresses for input markers. For details see note above. |
| Markers - PLC Base Out | This option is used to show the calculated the base PLC addresses for output markers. For details see note above and “Marker PLC base out” on page 119. |
| Registers - In size (bytes) | Defines the number of reserved bytes on the SM Controller’s communication module for the register in buffer. For details see “Register In size (bytes)” on page 119. |
| Registers - Out size (bytes) | Defines the number of reserved bytes on the SM Controller’s communication module for the register out buffer. For details see “Register Out size (bytes)” on page 120. |
| Registers - PLC Base In | This option is used to set the base PLC addresses for input registers. For details see note above. |
| Registers - PLC Base Out | This option is used to show the calculated the base PLC addresses for output registers. For details see note above and “Register PLC base out” on page 121. |
| Enable Timeout | Defines whether a time out should be used. When used the communication timeout can detect failure of the communication link. |
| Time Out (ms) | Sets the maximum communication timeout in multiples of 100 milliseconds, in case Enable Timeout is checked. For more information see “Timeout (ms)” on page 121 |
| Network delay (ms) | Displays the known lag in communication. For more information see “Network delay (ms)” on page 122. |

DCS Logical network properties

| | |
|---|--|
|  | <p>Notes:</p> <ul style="list-style-type: none">• The Modbus marker PLC addresses range from 1 to 65535.• The Modbus register PLC addresses range from 1 to 65535. Long Words and Floats get 2 PLC addresses assigned. The most significant value in the sequence is stored at the lowest storage address.• For a detailed description of all network properties see “Logical View property fields explained” on page 116. |
|---|--|

To access this window, select or create a “*DCS to SM Controller*” row in the **Logical View** and click **Properties** from the tools menu

| | |
|--|--|
| Master Node | Contains the name of the MODBUS device you want to connect. |
| Slave Node | Contains the name of the SM Controller you want to connect. |
| Protocol | Defines the Modbus protocol. |
| Route | Contains the default route; change to an alternative route if desired. |
| Device address | Set the <i>SM Controller</i> Modbus address: This is the address the SM Controller will respond to. Modbus addresses between 1 – 247 are accepted. For more information see “Communication via the Modbus protocol” on page 309. |
| Markers - In size (bytes) | Defines the number of reserved bytes on the SM Controller’s communication module for the marker in buffer. For details see “Marker In size (bytes)” on page 118. |

| | |
|---|--|
| Markers - Out size (bytes) | Defines the number of reserved bytes on the SM Controller's communication module for the marker out buffer. For details see "Marker Out size (bytes)" on page 119. |
| Markers - PLC Base In | This option is used to set the base PLC addresses for input markers. For details see note above. |
| Markers - PLC Base Out | This option is used to show the calculated the base PLC addresses for output markers. For details see note above and "Marker PLC base out" on page 119. |
| Registers - In size (bytes) | Defines the number of reserved bytes on the SM Controller's communication module for the register in buffer. For details see "Register In size (bytes)" on page 119. |
| Registers - Out size (bytes) | Defines the number of reserved bytes on the SM Controller's communication module for the register out buffer. For details see "Register Out size (bytes)" on page 120. |
| Registers - PLC Base In | This option is used to set the base PLC addresses for input registers. For details see note above. |
| Registers - PLC Base Out | This option is used to show the calculated the base PLC addresses for output registers. For details see note above and "Register PLC base out" on page 121. |
| Enable Timeout | Defines whether a time out should be used. When used the communication timeout can detect failure of the communication link. |
| Time Out (ms) | Sets the maximum communication timeout in multiples of 100 milliseconds, in case Enable Timeout is checked. For more information see "Timeout (ms)" on page 121 |
| Network delay (ms) | Displays the known lag in communication. For more information see "Network delay (ms)" on page 122. |

External Clocksource Logical network properties

A set of External Clocksource logical network properties are defined for each logical (peer to peer) connection between an External Clocksource and an SM Controller.

To access this window, select or create an "*External Clocksource to SM Controller*" row in the **Logical View** and click **Properties** from the tools menu.

Logical Network Properties

Master Node: External clock-source

Slave Node: SM Controller

Protocol: NTP

Route: PTP

Device Address: --

Markers

In size (bytes): 0

Out size (bytes): 0

PLC base in: 0

PLC base out: 0

Registers

In size (bytes): 0

Out size (bytes): 0

PLC base in: 0

PLC base out: 0

☒ Enable Timeout

Timeout (ms): 1000

Network delay (ms): 0

OK Cancel Help

| | |
|-----------------------|---|
| Master Node | Contains the name of the external Clocksource you want to connect. |
| Slave Node | Contains the name of the SM Controller you want to connect. |
| Protocol | Defines the NTP or the PTP protocol. For details see “PTP/NTP based time servers” on page 335. |
| Route | Contains the default route; change to an alternative route if desired. |
| Device address | Not used. |
| Markers | Not used. |
| - In size (bytes) | |
| - Out size (bytes) | |
| Markers | Not used. |
| - PLC Base In | |
| - PLC Base Out | |

| | |
|---------------------------|---|
| Registers | Not used. |
| - In size (bytes) | |
| - Out size (bytes) | |
| Registers | Not used. |
| - PLC Base In | |
| - PLC Base Out | |
| Enable Timeout | Defines whether a time out should be used. When used the communication timeout can detect failure of the communication link. |
| Time Out (ms) | Sets the maximum communication timeout in multiples of 100 milliseconds, in case Enable Timeout is checked. For more information see “Timeout (ms)” on page 121 |
| Network delay (ms) | Displays the known lag in communication. For more information see “Network delay (ms)” on page 122. |

Network Configurator component properties explained



Note:

Network components have both physical and logical view properties.

- the physical properties of a component are visible in the **Physical view**
 - the logical properties of a component are visible in the **Logical view**
-

This topic explains how you can view and edit the different physical view properties of the various Network Configurator components.

The following component properties are described:

- “Physical View properties explained” on page 105
- “Logical View property fields explained” on page 116

Related sections:

- “Configuring Physical View component properties” on page 72.
- “Configuring Logical View component properties” on page 92

Physical View properties explained

Baud Rate

This field is used in “Physical network properties” on page 90.



Notes:

1. A warning message pops-up and the communication line turns red in the network work area if the speed is set too low to transport the required network data within the available time frame.
 2. This option is not available when **Interface** is set to Ethernet.
-

This field contains speed setting of the network connection. The available options in the pull down menu differ for each interface.

Clock source allowed

This check box is used in the following Component Properties windows:

- “Safety Builder properties” on page 74
- “Experion server properties” on page 86
- “External Clocksource properties” on page 88



Attention:

Make sure that the time zone and day-light saving settings of this **device** match the time zone and daylight saving settings of various selected clock sources are identical..

It defines whether or not the use of this component as clock source is allowed.
See also “Clock source timeout” on page 106.

Clock source timeout

This property is used in the following Component Properties windows:

- “Safety Builder properties” on page 74
- “CEE Controller properties” on page 85
- “Experion server properties” on page 86
- “External Clocksource properties” on page 88

It defines the clock source time-out period, once Clock source allowed is activated. Values ranging from 1 min. to 30 hour can be chosen.

If no time synchronization takes place within this time-out period, an error is generated. The default time-out value set differs per selected device.

See also “Clock source allowed” on page 105.

Communication redundancy fail-over

This check box is shown in the following Component Properties windows:

- “Safety Builder properties” on page 74
- “CEE Controller properties” on page 85
- “Experion server properties” on page 86
- “DCS properties” on page 87
- “External Clocksource properties” on page 88

Communication redundancy fail-over is the automated capability of a device to switch over to a redundant or dormant communication path upon the failure or abnormal termination of the active path.

To determine which line is dormant and which is active a token is used by either the responder or the initiator of the communication, i.e. Safety Manager or the other system.

- When you choose **Safety Manager as the device controlling the fail-over**, you must **uncheck** the checkbox in the properties window of the device Safety Manager is connected to.

Safety Manager will swap paths roughly every ten seconds as long as the dormant path remains healthy.

If a path is diagnosed faulty, Safety Manager swaps to the remaining healthy path. A diagnostic message logs the communication failure. At the same time Safety Manager keeps trying the faulty path: As soon as the faulty path is found healthy again Safety Manager initiates a fail-back which results in both paths being used again.

- When you choose ***the other system as the device controlling the fail-over***, you must **check** the checkbox in the properties window of the device Safety Manager is connected to.
Safety Manager will wait for the device to switch paths in case a communication failure takes place.



Note:

For more information see “Communication redundancy based on the fail-over principle” on page 289.

This property can only be changed in the DCS properties, described in “DCS properties” on page 87.

Com Module

This location is used in the “SM Controller properties (physical) - tab: COM module x” on page 78.

It contains an overview of the used COM Module and their names (types).

COM Port

This property is used in the “SM Controller properties (physical) - tab: COM module x” on page 78 and in “Physical network properties” on page 90.

- When used in **SM Controller properties** - tab **General**, it contains the COM port connecting the SM Controller with the master network above.
Information shown here depends on the number of communication modules that are defined (see “SM Controller properties (physical) - tab: COM module x” on page 78):
 - In case of 1 communication module, you can choose [1A, 1B] or [1C, 1D], depending on the network protocol.
 - In case of 2 communication modules, you can choose [1A, 1B, 2A, 2B] or [1C, 1D, 2C, 2D], depending on the network protocol.
- When used in **Physical network properties** it contains the COM port used on the master device.

Controller Architecture

This property is used in the “SM Controller properties (physical) - tab: General” on page 75.



Attention:

Changes to this field can have implications for the availability of your project.

This property defines the SM Controller architecture: It can be either **Non-redundant** or **Redundant**.

Controller Description

This field is used in the “SM Controller properties (physical) - tab: Additional information” on page 84.

It contains a short description of the controller. The maximum length of the controller description is 255 characters.

Controller Name

This property is used in the “SM Controller properties (physical) - tab: General” on page 75.

It contains the name of the SM Controller. Every SM Controller in your configuration must have a unique name.



Note:

You can enter the Controller Name directly in this text field and continue by choosing a Project File Directory, or enter the Controller Name while choosing a Project File Directory.

Controller Node No.

This property is used in the “SM Controller properties (physical) - tab: General” on page 75.

This property defines the node number for the SM Controller.

SM Controllers must have a non-conflicting node number, in the range of 1 to 63, when communicating via SafeNet.

Safety Builder automatically disables node numbers occupied by other SM Controllers, communicating via the same SafeNet.

When SM Controllers do not communicate via SafeNet it is allowed (but not advised) to assign the same node number to multiple SM Controllers in the plant.

Customer (tab)

This tab is used in the window “Plant properties” on page 72.

It provides access to contact information about the end user of the system.

Customer Reference

This field is used in the “SM Controller properties (physical) - tab: Additional information” on page 84.

It contains the identification reference of the end user. The contents of this field are supplied by Honeywell.

Database Path

This property is used in the window “Plant properties” on page 72.

It identifies the location where the database for the current plant is stored on disk. The Database Path can be defined by clicking on the “...” button and choosing a name and location for the plant. This field must be filled in when a new plant is created.

If you do not enter a **Plant name**, you can use this field to open an existing plant database.

Date Format

This property is used in the window “Plant properties” on page 72.

It identifies the format of the dates shown in Safety Builder.

Degree Type

This property is used in the window “Plant properties” on page 72.

It identifies whether temperatures are to be displayed in Kelvin, degrees Fahrenheit or degrees Celsius.

Device name

This property is used in the following Component Properties windows:

- “Safety Builder properties” on page 74
- “CEE Controller properties” on page 85
- “Experion server properties” on page 86
- “DCS properties” on page 87
- “External Clocksource properties” on page 88

It identifies the name of the device running the component. Every component in your configuration must have a unique name.

Diagnostic Test Interval

This property is used in the “SM Controller properties (physical) - tab: General” on page 75.



Attention:

Changes to this field can have implications for the availability of your project.

This property defines the Diagnostic Test Interval (measured in seconds).

Honeywell (tab)

This tab is used in the window “Plant properties” on page 72.

It provides access to contact information about the Honeywell organization supporting the plant.

Honeywell (E) SID

This field is used in the “SM Controller properties (physical) - tab: Additional information” on page 84.

It contains the Honeywell project identification code. The contents of this field are supplied by Honeywell.

Interface

This field is used in “Physical network properties” on page 90.

It identifies the interface used to connect the device to the network. Available options are:

- RS485,
- RS422,
- RS232 and
- Ethernet.

IP Address

This property is used in the following Component Properties windows:

- “External Clocksource properties” on page 88.
- “SM Controller properties (physical) - tab: COM module x” on page 78



Tip:

When assigning IP addresses check with your organization's network administrator to identify specific addresses that may be used at your facility. While there will be no conflict with Internet networks, your organization may already use one or more of the private networks.

Below steps assist in assigning valid IP address ranges:

1. Only assign IP addresses within the IP address space reserved for private networks.
 2. Follow the Experion FTE addressing guidelines when assigning IP addresses as part of an FTE network (for details see the Experion User Guides).
-

This property contains the IP address of the device.

Logo

This field is used in the “SM Controller properties (physical) - tab: Additional information” on page 84.

You can use the **Logo** field to refer to an image that will be used on the prints of your configuration.

Click on the “...” button to open a window where you can open this logo.

Max SOE ID

This field is used in “SM Controller properties (physical) - tab: SOE” on page 80.

Note:

The Min SOE ID and Max SOE ID determine the range of SOE ID's. The smallest SOE ID range is 2.

This field contains the highest SOE ID for this SM Controller.

- The **Min SOE ID** and **Max SOE ID** determine the range of SOE ID's. The smallest SOE ID range is 2.

The **Max SOE ID**:

- cannot overlap SOE ID ranges of other SM Controllers
- must be at least 2 counts larger than the Min SOE ID.

See also:

- “SOE enable” on page 115
- “Min SOE ID” on page 112

Min SOE ID

This field is used in “SM Controller properties (physical) - tab: SOE” on page 80.



Note:

The Min SOE ID and Max SOE ID determine the range of SOE ID's. The smallest SOE ID range is 2.

This field contains the lowest SOE ID for this SM Controller.

- The **Min SOE ID**:
 - cannot be lower than 16;
 - cannot overlap SOE ID ranges of other SM Controllers;
 - must be at least 2 counts smaller than the Max SOE ID.

See also:

- “SOE enable” on page 115
- “Max SOE ID” on page 111

Network Name

This field is used in “Physical network properties” on page 90.



Note:

Every network element in your configuration must have a unique name.

It contains the name of the network.

On-line Modification

This check box is used in the “SM Controller properties (physical) - tab: General” on page 75.

It toggles the On-line Modification feature. For more information see the *On-line Modification Guide*.

Parity

This field is used in “Physical network properties” on page 90.



Notes:

This option is not available when **Interface** is set to Ethernet. If this option is shaded, the current value is the only one possible for the chosen network configuration.

It contains the parity bit used for communication. Available options: None, Odd and Even.

Plant (tab)

This tab is used in the window “Plant properties” on page 72.

It provides access to contact information about the plant Safety Manager is installed.

Plant Name

This property is used in the window “Plant properties” on page 72.

It identifies the name of the plant. Every plant in your configuration must have a unique name.

You can enter the Plant Name directly in this text field and continue by choosing a **Database Path**, or enter the Plant Name while choosing a Database Path.

Plant Wide Properties

This group of properties is used in the window “Plant properties” on page 72.

These properties will be enabled only when the plant is open for configuration. The following properties are part of this group:

- “Symbol Library” on page 115
- “Degree Type” on page 109
- “Date Format” on page 109
- “Time Zone” on page 116

Principal Information

This field is used in the “SM Controller properties (physical) - tab: Additional information” on page 84.

It contains Controller specific information that will be used on the prints of your configuration.

Project File Directory

This property is used in the “SM Controller properties (physical) - tab: General” on page 75.

It identifies the location where the application files for the current controller are stored on the disk.

The Project File Directory can be defined by clicking on the “...” button and choosing a name and location for the controller. This field must be filled in when a new controller is created.

If you do not enter a **Controller name**, you can use this field to open an existing controller file.

Real time clock source

This location is used in the “SM Controller properties (physical) - tab: Clock Source” on page 82.



Attention:

All accessible clock sources *must* be set to the same time zone!

In this area you will find priority level settings for different clock sources.

By default Clock Source Priority 1 will be used. If Clock Source Priority 1 fails after the time-out, Clock Source Priority 2 will be used, etc.

Only devices that are connected to the selected Controller in the Logical View and that have the option **Clock Source Allowed** checked on are available for selection in these pull-down menus.

Safety Integrity Level

This property is used in the “SM Controller properties (physical) - tab: General” on page 75.



Attention:

Changes to this field can have implications for the availability of your project.

This property specifies the level of safety performance (SIL) for the overall system.

For more information see the *Safety Manual*.

Signal Encoding

This field is used in “Physical network properties” on page 90.



Notes:

This option is not available when **Interface** is set to Ethernet. If this option is shaded, the current value is the only one possible for the chosen network configuration.

This field sets the signal encoding used for RS485 and RS422 communication. Available option is None.

SOE collection

This check box is used in the “Experion server properties” on page 86.

It assigns this device as SOE collection device.

See also:

- “SOE enable” on page 115
- “Min SOE ID” on page 112
- “Max SOE ID” on page 111

SOE enable

This field is used in “SM Controller properties (physical) - tab: SOE” on page 80.

It enables the collection and communication of events by the SM Controller.

See also:

- “SOE collection” on page 115
- “Min SOE ID” on page 112
- “Max SOE ID” on page 111

Stop Bits

This field is used in “Physical network properties” on page 90.



Notes:

This option is not available when **Interface** is set to Ethernet. If this option is shaded, the current value is the only one possible for the chosen network configuration.

It contains the number of stop bit used in communication over current network. Available options are 1 or 2.

Symbol Library

This property is used in the window “Plant properties” on page 72.

This property sets the FLD size for the Application Editor. All available symbol libraries offer the same functionality and differ only in size and layout.

Transport Protocol

This field is used in “Physical network properties” on page 90.

It contains the communication protocol used by this network.

This protocol changes automatically depending on the chosen setting for **Interface**.

Time Zone

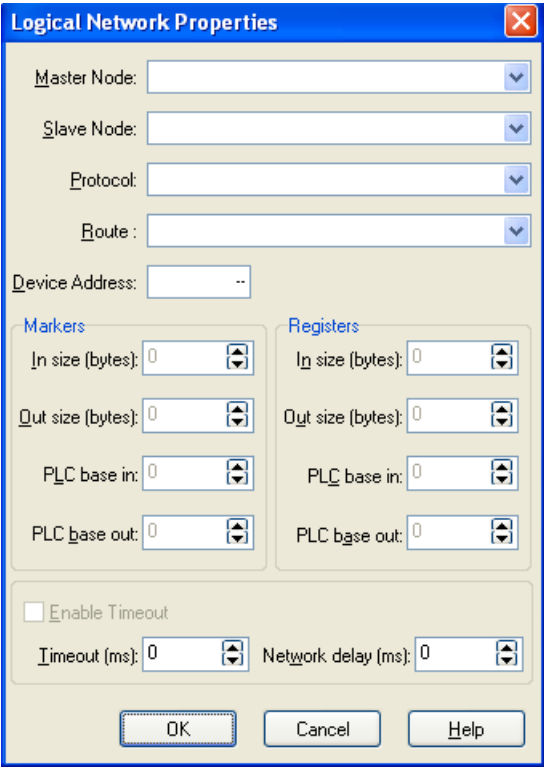
This property is used in the window “Plant properties” on page 72.

It identifies the time zone applied by SM Controllers in the Plant, when synchronizing with an external clock source.

(See also “External Clocksource properties” on page 88.)

Logical View property fields explained

Figure 14 The default Logical Network Properties window



Depending on the type of logical connection (protocol) the **Logical Network Properties** window, as shown in Figure 14 on page 116, may contain the following properties fields:

Master Node

The network component that initiates communication with its peer.

Master node is available in the following logical network properties:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100
- “External Clocksource Logical network properties” on page 102

Slave Node

The network component that waits for its peer to initiate communication.

Slave node is available in the following logical network properties:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100
- “External Clocksource Logical network properties” on page 102

Protocol

Defines the communication protocol used between the master and slave node.

Protocol contains the protocol options used to communicate between the connected components.

The options shown in the list box are limited to the protocols supported by both components.

Protocols are available in the following logical network properties:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100
- “External Clocksource Logical network properties” on page 102

Route



Tip:

Scale the window if only part of the Route is displayed.

This list box shows the selected communication path to make the logical connection. With the dropdown arrow you can select another (e.g. less loaded or less critical) link.

Route is available in the following logical network properties:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100
- “External Clocksource Logical network properties” on page 102

Device Address

This text box contains the communication address used by the master node or the slave node.

Depending on the protocol used the **Device Address** is either

- the device ID of the slave (SM Controller), used by the master to address the slave or
- the device ID of the master, as a means to the slave (SM Controller) to identify the master.

To change the device address click the value in the text box and enter a new value.

- If a device address field contains -- an alternative addressing method is used.

Marker In size (bytes)

This field is used in:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100

This field is used to reserve memory space on the communication module.

It defines the size of the marker *in* buffer of the (master) SM Controller (the amount of bytes that are reserved in memory for Digital Input Point data for use over the selected network).

| | |
|---------|--|
| Example | Entering 100 corresponds to 100 bytes = 100x8 digital input signals. |
|---------|--|

Marker Out size (bytes)

This field is used in:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100

This field is used to reserve memory space on the communication module.

It defines the size of the marker **out** buffer (the amount of bytes that are reserved in memory for Digital Output Point data for use over the selected network).

| | |
|---------|---|
| Example | Entering 100 corresponds to 100 bytes = 100x8 output input signals. |
|---------|---|

Marker PLC base in

This field is used to set the base PLC address for input markers.

To change click the arrows or enter a new value.

For more information about PLC addresses and address ranges see “PLC address” on page 405.

Marker PLC base out

This field is used to show the calculated base PLC address for output markers. The address is calculated as follows:

$$\text{PLC base out} = \text{PLC base in} + 8 \times \text{In size (bytes)}$$

For more information about PLC addresses and address ranges see “PLC address” on page 405.

Register In size (bytes)

This field is used in:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100

This field is used to reserve memory space on the communication module. It defines the size of Register **in** buffer (the amount of bytes that are reserved in memory for Binary Input Point data for use over the selected network).

Example Entering 100 corresponds to 100 bytes. 100 bytes corresponds to:

- 100 BI type byte or
 - 50 BI type word (each 2 bytes) or
 - 25 BI type long word (each 4 bytes) or
 - 25 BI type float (each 4 bytes) or
 - a combination of above
-

Register Out size (bytes)

This field is used in:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “CEE Controller logical network properties” on page 96
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100

This option is used to reserve memory space on the communication module. It defines the size of Register **out** buffer (the amount of bytes that are reserved in memory for Binary Output Point data for use over the selected network).

Example **Example:** entering 100 corresponds to 100 bytes. 100 bytes corresponds to:

- 100 BO type byte or
 - 50 BO type word (each 2 bytes) or
 - 25 BO type long word (each 4 bytes) or
 - 25 BO type float (each 4 bytes) or
 - a combination of above
-

Register PLC base in

This field is used to set the base PLC address for input registers.

To change click the arrows or enter a new value.

For more information about PLC addresses and address ranges see “PLC address” on page 405.

Register PLC base out

This field is used to show the calculated base PLC address for output registers. The address is calculated as follows:

$$\text{PLC base out} = \text{PLC base in} + \frac{\text{PLC in size (bytes)}}{2}$$

For more information about PLC addresses and address ranges see “PLC address” on page 405.

Enable Timeout

This checkbox is used in:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100
- “External Clocksource Logical network properties” on page 102

When checked it identifies that the **Timeout** function is used.

Note:

Communication timeout is mandatory for SafeNet to detect possible failures in the communication. You cannot disable the timeout.

See also “Timeout (ms)” on page 121.

Timeout (ms)

This field is used in:

- “Safety Builder logical network properties” on page 93
- “SafeNet logical network properties” on page 95
- “Experion Logical network properties” on page 98
- “DCS Logical network properties” on page 100
- “External Clocksource Logical network properties” on page 102

This field contains the maximum communication timeout in multiples of 100 milliseconds.

Typical timeout values are:

- 500–20 000 ms for SafeNet configurations

- 500–180 000 ms for other configurations

Network delay (ms)



Note:

If **Timeout** is enabled the network delay cannot be greater than the configured timeout.

This field contains the expected network delay (lag) in ms. You can enter a value between 0 ms and 32767ms, 0 ms is the default value.

Network delay forces the SM Controller to wait before repeating its communication burst in case the burst is not immediately acknowledged by the receiver:

If a communication burst is not acknowledged within a certain timeframe, the sender usually repeats the communication, assuming the first burst is lost.

Especially when having relatively slow communication media, such as RS232 or satellite connections, entering an anticipated network delay helps preventing blockage of the communication channel with repeated communication bursts.

Hardware Configurator

A Safety Manager configuration comprises one or more cabinets with chassis filled with modules.

This section covers the following topics:

| Section | See |
|------------------------------------|----------|
| Starting the Hardware Configurator | page 123 |
| Hardware Configurator menu | page 125 |
| Toolbars | page 127 |
| Modules bar | page 128 |
| Using Hardware Configurator | page 128 |
| Set Controller properties | page 129 |
| Setup the cabinet assembly | page 129 |
| Configuring Chassis | page 130 |
| Modules and slots | page 131 |
| Print | page 132 |
| Find Dialog | page 133 |
| Hardware component properties | page 133 |

Starting the Hardware Configurator



Notes:

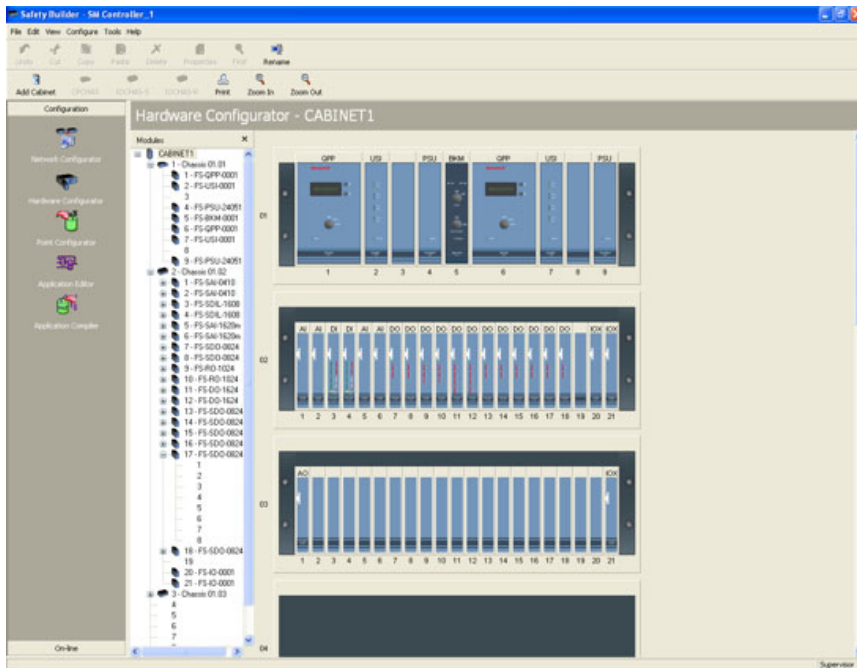
1. Hardware Configurator can only be started after you create a network and select a controller in the Network Configurator. (See “Selecting an SM Controller” on page 61.)
2. If you get a popup stating `exclusive access is denied` see “Working in a multi user environment” on page 124.

To start Hardware Configurator, you either:

- Click the icon in the outlook bar
- Open the corresponding menu via the menu bar (**Tools > Configuration > Hardware Configurator**)
- Press the shortcut keys **Alt, T, C, H**.

The Hardware Configurator screen appears, resembling Figure 15 on page 124.

Figure 15 Hardware Configurator screen



This program window consists of the following sections:

- The menu bar, toolbars, outlook bar and status bar.
For a description of these bars see “Screen layout” on page 27.
- The right section, the work area, shows a graphical layout of the current Safety Manager configuration.
- The left section, the Explorer bar, shows an hierarchical overview of the Safety Manager configuration.

Working in a multi user environment



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
2. To give up exclusive access to an SM Controller access the **Network Configurator**.
3. To give up shared access exit the tool or function that demands shared access.

To give up all access you can close the file (click **File>Close** from the menu bar).

When you try to access the SM Controller with multiple users simultaneously, access via this tool may be denied and you get a popup stating either:

Access is denied, please try again later.

Exclusive access is denied, please try again later.

- If the Plant database is opened for exclusive use by someone using Network Configurator, your access to this tool is denied.
- If the SM Controller database is opened by someone, using this or a similar tool, your access to this tool is denied.

In above cases, you cannot continue until the “denied access” lock is relieved by the other user(s).

For more information see also “Multi user environment” on page 36.

Hardware Configurator menu

Below list shows the Safety Builder Hardware Configurator menu structure.

The shortcut access key combinations, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also “Keyboard shortcut and access keys” on page 32.

| Menu item | Description |
|---------------------|--|
| File | |
| > <i>Close</i> | Closes the Hardware Configurator. |
| > <i>Print</i> | Print the current network configuration. For more information see “Hardware component properties” on page 133. |
| > <i>Exit</i> | Exits Safety Builder. |
| Edit | |
| > <i>Undo</i> | Undo the last action. Safety Station supports multiple undo's. |
| > <i>Cut</i> | Deletes the currently selected object and adds it to the copy buffer. |
| > <i>Copy</i> | Copy the value of current selection into the copy buffer. |
| > <i>Paste</i> | Paste the value of the copy buffer at the currently selected location. |
| > <i>Delete</i> | Deletes the currently selected object. |
| > <i>Properties</i> | View or edit the properties of the selected component. |

| | |
|------------------------------------|---|
| > F ind | Opens up the find dialog (see “Find Dialog” on page 133). |
| > R ename | Renames cabinet name. This function is only available when a Cabinet is selected (in the Explorer bar). |
| View | |
| > T oolbars | Toggles display of the available toolbars. |
| > O utlook bar | Toggles display of the Outlook bar. |
| > A udit Trail Viewer | Launches the Audit Trail Viewer. For more information see “Audit Trail” on page 276. |
| > M odules bar | Toggles display of the Modules bar. |
| > Z oom In | Zooms in on the work area. |
| > Z oom Out | Zooms out on the work area. |
| > C ompilation Log File | Opens the Application Compiler log file. |
| Configure | |
| > A dd Cabinet | Add a new cabinet to configuration (see “Adding cabinets” on page 129). |
| > C ontroller properties | View and modify properties of current controller (see “Set Controller properties” on page 129). |
| > CPCHAS | Add a Controller chassis to the configuration (see “Configuring Chassis” on page 130). This option is only available when you click on a position in the Explorer bar or the work area where a chassis of this type can be placed. |
| > IOCHAS-S | Add a Non-redundant IO chassis to the configuration (see “Configuring Chassis” on page 130). This option is only available when you click on a position in the Explorer bar or the work area where a chassis of this type can be placed. |
| > IOCHAS-R | Add a Redundant IO chassis to the configuration (see “Configuring Chassis” on page 130). This option is only available when you click on a position in the Explorer bar or the work area where a chassis of this type can be placed. |

Tools

| | |
|-------------------------|--|
| > C onfiguration | Displays a sub menu with available configuration tools. For an overview see “Safety Builder configuration tools” on page 41. Unavailable tools will appear shaded. |
| > O n-line | Displays a sub menu with available on-line tools. Unavailable tools will appear shaded. |
| > P assword | Launches the Security tool (see “Security” on page 281). |
| > O ptions | Enables you to set general program options (see “Options” on page 274). |

Help

| | |
|-------------------------------|---|
| > S afety Builder help | Launches the Safety Builder Help function. |
| > A bout | Shows current version and license of the program. |

Toolbars

**Note:**

A toolbar only shows the most used tool functions and components. Some tool functions and components have to be accessed via an item in the Menu bar.

A toolbar contains a subset of tools or components that can be used by the active program.

Multiple toolbars can be active at the same time.

Hardware Configurator Components

The Hardware Configurator Components toolbar contains buttons to add components and buttons to zoom and print.

Click **View>toolbars>Hardware Configurator Components** to toggle the Hardware Configurator Components toolbar.

Hardware Configurator Operations

The Hardware Configurator Operations toolbar contains the most common functions.

Click **View>toolbars>Hardware Configurator Operations** to toggle the Hardware Configurator Operations toolbar.

Modules bar

The Modules bar is an Explorer bar as defined in “Explorer bar” on page 30. You can use it to get an hierarchical overview of the hardware configuration of the selected Controller.

The Modules bar:

- highlights the component you have selected,
- provides you access to the main tool functions related, by right clicking a component.

Using Hardware Configurator



Tip:

For more information on hardware planning, see *Planning and Design Guide*.

With aid of Hardware Configurator you set up Safety Manager hardware, such as cabinets, chassis, and modules.

To configure the hardware of Safety Manager you need to perform the following steps:

- 1 From Network Configurator select the Safety Manager in the Explorer bar.
- 2 Open Hardware Configurator.
- 3 Set the properties of the Controller.
- 4 Add and set up the cabinets in which the Safety Manager will be housed.
- 5 Add a Controller chassis.
- 6 Add redundant and/or non-redundant IO chassis to the cabinets.
- 7 Allocate IO modules to the IO chassis.
- 8 Set the IO module properties.

Hardware Configurator shortcut keys

Besides the shortcut keys listed in “Keyboard shortcut and access keys” on page 32, the following shortcut keys are activate when you use the Hardware Configurator:

- **F2** opens the rename function of the active component.

Set Controller properties

A number of Controller properties have been set in the Network Configurator. The remaining -network independent- properties are to be defined before the hardware is assembled.



Note:

The IO bus configuration settings of the Controller determine the availability of redundant and/or non redundant IO chassis.

The **Controller properties** dialog has three tabs that you need to verify:

- “Controller properties - General” on page 134
- “Controller properties - Temperature limits” on page 135
- “Controller properties - IO bus configuration” on page 136

To open the Controller properties, click **Configure>Controller properties**.

Setup the cabinet assembly

The following rules apply to Safety Manager cabinets:

1. create at least one cabinet and maximal five cabinets
2. each cabinet assembly must contain one Controller chassis
3. each cabinet assembly may contain a number of IO chassis (optional)

A cabinet may contain:

- up to 8 IO chassis with a Controller chassis installed or
- up to 9 IO chassis with no Controller chassis installed.

Adding cabinets

To add a cabinet you must open the Cabinet Properties:

Click the **Add cabinet** button in the Hardware Configurator Components toolbar or select **Configure > Add cabinet** in the menu to add a cabinet to the configuration.

- Adding a cabinet with number 1 will add a cabinet to the left
- Adding a cabinet with a different number will add a cabinet to the right

For details see “Cabinet properties” on page 137.

Deleting cabinets

You can delete a cabinet by right-clicking it in the Explorer bar, and then selecting **Delete**.

The cabinet containing the Controller can not be deleted.

Renaming cabinets

You can change the name of a cabinet by right-clicking it in the Explorer bar, and then selecting **Rename**

The name of a cabinet must be unique in a Plant.

Configuring Chassis

A chassis is a holder for modules.

Depending on your configuration the following chassis are available:

- Controller chassis (CPCHAS),
- Non-redundant IO chassis (IOCHAS-S),
- Redundant IO chassis (IOCHAS-R).

Adding chassis



Attention:

1. The first chassis you place is always the Controller chassis.
 2. To add a redundant IO chassis, a redundant IO bus is needed, and to add a non-redundant IO chassis, a non-redundant IO bus is needed. Defining an IO bus as redundant or non-redundant is described in “Controller properties - IO bus configuration” on page 136
-

To add a chassis,

- 1 Click a free location in a cabinet.
- 2 The toolbar shows the available chassis for the cabinet that you are configuring (**CPCHAS**, **IOCHAS-S** or **IOCHAS-R**).
- 3 To add the available chassis, right-click an empty chassis position in the work area or the outlook bar and select the chassis you want to add, or drag the chassis icon from the toolbar to the appropriate place in the work area.
- 4 When adding IO chassis you can go to “IO chassis properties” on page 137 to modify the IO bus that controls the IO chassis.

Moving chassis

You can move an entire chassis by selecting it in the work area and then dragging it to the desired empty chassis. When you move a chassis, all its contents (for example IO modules) will also be moved.

You can also move a chassis by selecting it in the outlook bar or the work area, then right click and choose **Cut**. Then go to the desired location and right click and choose **Paste**.

Deleting chassis

You can delete a chassis by right-clicking it in the outlook bar or the work area and then select **delete**.

If you delete a chassis that contains IO modules, these modules will also be deleted. If the modules have points allocated to them, these points will be de-allocated.

Safety Builder prompts when underlying IO modules and/or IO points are deallocated.

Modules and slots



Note:

A Controller chassis contains CP modules when added, an IO chassis will have no IO modules when added

Slots are placeholders for modules. Depending on the type, a module occupies one or more slots.

An IO chassis can contain 18 modules. A redundant IO module typically occupies two adjacent slots.

Adding IO modules

If an IO chassis has empty slots, modules can be added to them. To do so, right-click in the chassis and select the desired module.

Safety Builder only displays the modules that are available for the selected location.

After placing a (redundant) IO module, you can modify its properties. See “IO Module properties” on page 139 for details.

Deleting IO modules

To delete modules, click the module and click the delete button in the Hardware Configurator Operations toolbar.

Alternatively you may also hit **delete** on your keyboard or right click the module and select delete from the popup menu.

If the IO modules you are deleting have points allocated to them, these points will be de-allocated.

Safety Builder prompts you when underlying IO points are deallocated.

Adding and deleting CP modules

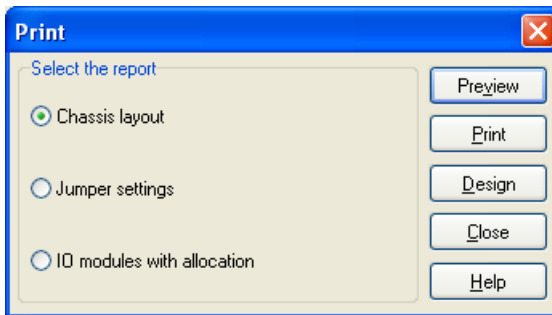
CP modules are added and deleted in the same manner as IO modules.

A number of modules however are mandatory for Safety Manager to function; they cannot be modified unless the Controller properties are modified (see “Controller properties - General” on page 134.)

Print

This windows allows you to print the hardware configuration in several report types.

To access this window select **File > Print** from the menu.



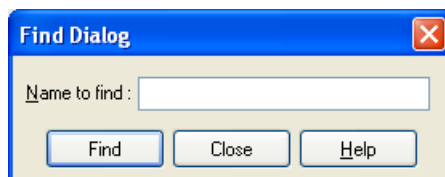
- | | |
|------------------------|---|
| Chassis layout | Selects printing of chassis layout. This option is used to print the IO tag strips which are used on the IO chassis. |
| Jumper settings | Selects printing of jumper settings. This option is used to print the jumper settings of IO chassis address. |

| | |
|-----------------------------------|---|
| IO Modules with allocation | Selects printing of IO modules with allocation. This option is used to print a graphical chassis layout with IO modules and tag numbers. |
| Preview | Shows a preview of the selected report. |
| Print | Prints the selected report. |
| Design | Opens the report design utility. For more information on using this utility, see the user manual for FastReport (version 2.5). |
| Close | Close the print dialog without printing. |
| Help | Launches the Safety Builder Help function. |

Find Dialog

You can use the find function to locate hardware components by name. To access the find dialog:

1. First select a cabinet or chassis in the Explorer Bar, then
2. Select **Edit > Find** in the menu or press CTRL+F.



| | |
|---------------------|---|
| Name to find | The name of the hardware unit you want to search. <ul style="list-style-type: none"> • The search is case sensitive: searching for “test” will not find “Test”. • Use the asterisk sign (*) as a wildcard: searching for “test*” will find “test” but also “test 1” and “test 2”. |
| Find | Start the search |

Hardware component properties

This section describes how you can view and edit the different properties of the various hardware components.

Controller properties

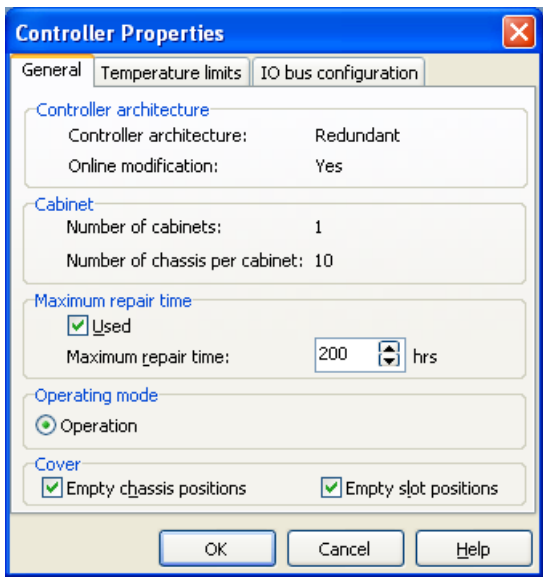
In the **Controller properties** dialog box, you can view the properties of the Controller that are hardware specific. Note that other properties of the Controller

are set in the Network Configurator. For details see “Physical SM Controller properties” on page 75 and “Creating a logical network” on page 52.

Controller properties - General

In this window, you can view and edit the general properties of the selected controller.

To access this window, open it via the menu **Configure > Controller properties** and select the **General** tab.



| | |
|--------------------------------|---|
| Controller architecture | Information about the Controller Architecture (Non-redundant or redundant) of the controller. This information can not be modified by the user here. |
| On-line modification | Show whether or not on-line modification is allowed. This information can not be modified by the user here. |
| Cabinet | The number of cabinets connected to the controller. The number of chassis per cabinet. Both can not be modified by the user here. |
| Maximum repair time | Activates the Maximum repair time functionality and the settings for its duration. This is the time a Safety Manager continues operating after fault detection in a safety related function. If the fault is not cleared within this period, Safety Manager automatically shuts down. |
| Operating mode | The operation mode is used for “daily use” of Safety Manager. |

Cover

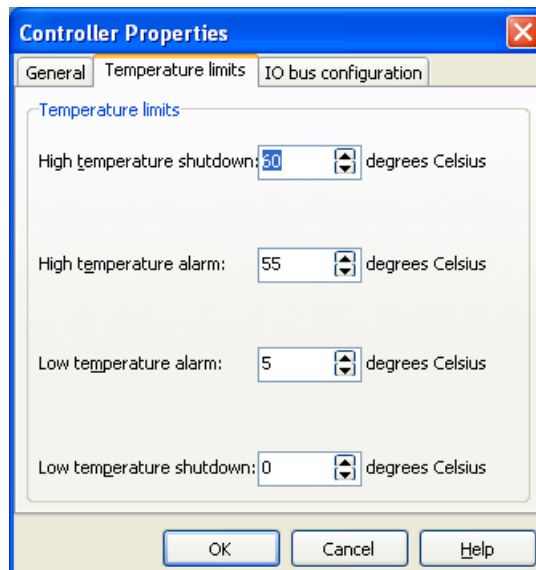
Here you can mark if empty chassis or slot positions are covered by a cover plate. These settings do not affect functionality or safety of the configuration but are there for report purposes.

Controller properties - Temperature limits**Warning:**

1. You are advised not to set the *High* and *Low temperature shutdown* values outside the approved operating range of -5°C — 70°C (23°F — 158°F) as the system may become unstable when operating beyond these temperature ranges.
2. Take additional temperature limitations into account when defining temperature shutdown limits. For details see the module specifications as described in the *Hardware Reference*.

In this dialog box, you set the temperature limits for alarm and shutdown conditions related to the operating temperature measured inside the CP Chassis.

To access this window, open it via the menu **Configure > Controller properties** and select the **Temperature limits** tab.

**High temperature shutdown**

The temperature limit above which the Control Processor shuts down.

The default setting is $+60^{\circ}\text{C}$ (140°F), the maximum setting is 85°C (185°F), the minimum setting is above the High temperature alarm.

- High temperature alarm

The temperature limit above which the Control Processor gives an alarm.

The default setting is +55°C (131°F), the minimum setting is 35°C (95°F), the maximum setting is below the *High temperature shutdown*.
- Low temperature alarm

The temperature limit below which the Control Processor gives an alarm.

The default setting is 5°C (41°F), the maximum setting is 15°C (59°F), the minimum setting is above the *Low temperature shutdown*.
- Low temperature shutdown

The temperature limit below which the Control Processor shuts down.

The default setting is 0°C (32°F), the minimum setting is -20°C (-4°F), the maximum setting is below the *Low temperature alarm*.

Controller properties - IO bus configuration

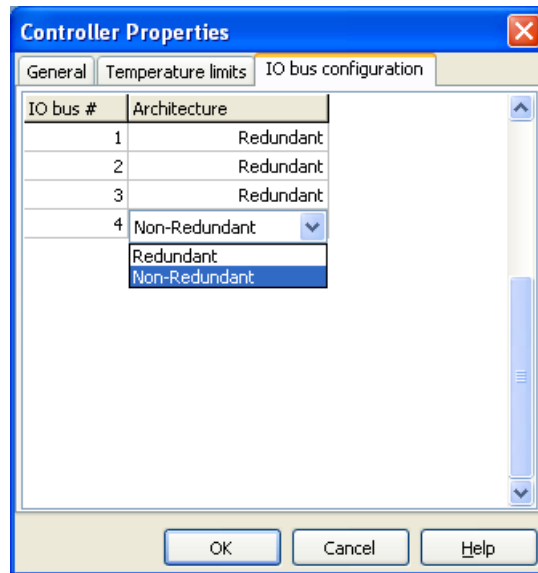
With this tab, you define the redundancy settings for every IO bus.

To access this window, open it via the menu **Configure > Controller properties** and select the **IO bus configuration** tab.

When setting an IO bus to non-redundant, you must start with the highest IO bus number (4). The second non-redundant IO bus must be number 3, and so on. This leads to the following possible configurations:

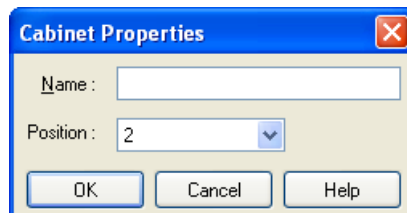
Table 3 IO bus configurations

| Number of redundant buses: | | | | | |
|---------------------------------|---|---|---|---|---|
| | 4 | 3 | 2 | 1 | 0 |
| IO #1 | R | R | R | R | N |
| IO #2 | R | R | R | N | N |
| IO #3 | R | R | N | N | N |
| IO #4 | R | N | N | N | N |
| R = Redundant N = Non-Redundant | | | | | |



Cabinet properties

To access this window, Click the **Add cabinet** button in the Hardware Configurator Components toolbar or select **Configure > Add cabinet** in the menu.



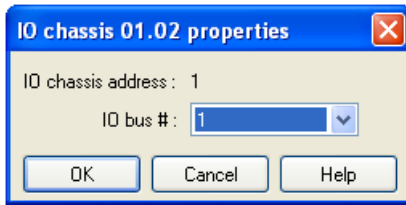
Name The name of the cabinet. This must be a plant-wide unique name.

Position The position of the cabinet. You can place the new cabinet before (choose 1) or after (choose the highest number) the existing cabinets.

IO chassis properties

You can use this window to change and view the IO chassis properties.

To access this window right-click a chassis in the Explorer bar or the work area and select **properties**. A window similar to the following will appear:



IO chassis address Shows IO chassis address.

IO bus # Defines the IO bus that interconnects the IO chassis with the SM Controller. For single chassis you can only choose single busses, for redundant chassis you can only choose redundant busses. For information on how to define the redundancy of an IO bus, see “Controller properties - IO bus configuration” on page 136.

CP Module properties



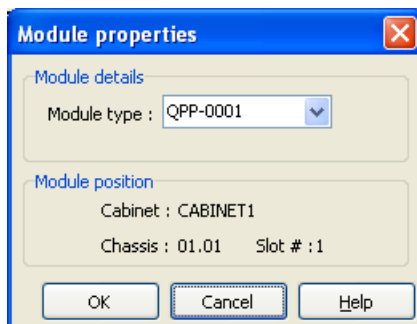
Note:

When a QPP-0001 is selected but a QPP-0002 is placed, the module switches back to the “QPP-0001 compatible mode”.

This window contains module type information displayed in a drop-down box. For most modules this information is shaded and cannot be edited.

- For the QPP module the drop-down box allows you to select a QPP-0001 or a QPP-0002. QPP-0001 is the default choice. QPP-0002 is optional and has enhanced functions.

The CP Module properties window shows the module name, module type and where it is located in the cabinet. To access this window, right-click the module in the outlook bar or the work area and click **Properties**.



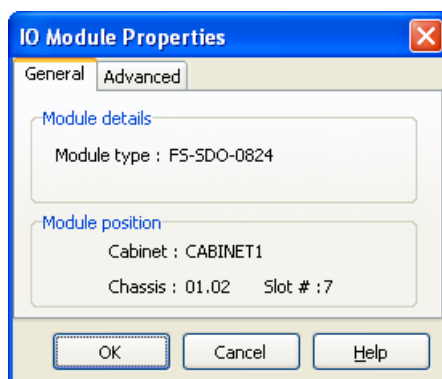
IO Module properties

In the **IO Module properties** dialog box, you can view the properties of the selected IO module and indicate or view whether the module should be test enabled or ELD monitored (depending on the IO module, some settings may not be available). In addition, you can define the voting settings (some settings may not be customizable).

IO Module properties - General

This tab is available for all IO modules.

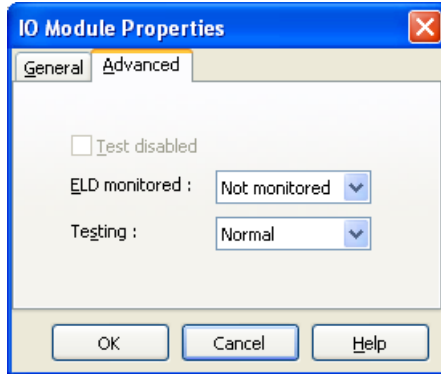
This tab only displays information and cannot be edited. It shows the IO module name, module type and where it is located in the cabinet. To access this window, right-click the module in the outlook bar or the work area, click **Properties** and select the **General** tab.



Module properties - Advanced

This tab is only available for IO modules, and not for CP modules or IO extenders.

To access it, right-click the module in the outlook bar or the work area, click **Properties** and select the **Advanced** tab.



- Test disabled** When this option is checked, the testing of the selected module is disabled.
- This option is only available for Analog Outputs.
- ELD monitored** Defines the monitoring of Earth Leakage Detection (ELD). Options are **Not monitored**, **Floating** and **Grounded**. This option only applies for modules supporting ELD (see *Hardware Reference*).
- Testing** The type of voting used in this module. Available options are **Normal** and **1oo2d**, depending on the chosen architecture.

Point Configurator

Points are variables containing (field) values that can be processed by a Control Processor. Points need to be configured in the Point Configurator before they can be processed.

To configure points, you need to set their properties and allocate them to IO channels or communication channels.

With a Safety Manager selected you can use Point Configurator to:

- Create points.
- Allocate, modify and view points.
- Import and Export points.
- Delete points.
- Define and change the layout of point Views for on-screen and in reports.
- Create hard copies (reports) of point Views.


This section covers the following topics:

| Topic | See |
|---------------------------------|----------|
| Starting the Point Configurator | page 142 |
| Point Configurator menu | page 144 |
| Toolbars | page 146 |
| Views bar | page 147 |
| Using the Point Configurator | page 147 |
| Working with Views | page 148 |
| Configuring Views | page 152 |
| Working with points | page 156 |
| Configuring a point | page 158 |
| Importing and exporting points | page 162 |
| Find Dialog | page 164 |
| Print | page 166 |
| Point properties | page 167 |

Starting the Point Configurator

To start the Point Configurator from Safety Builder:

- Click its icon in the **Outlook bar**,
- Click **Tools > Configuration > Point Configurator** from the **Menu bar**
- Press the shortcut keys **Alt, T, C, P**

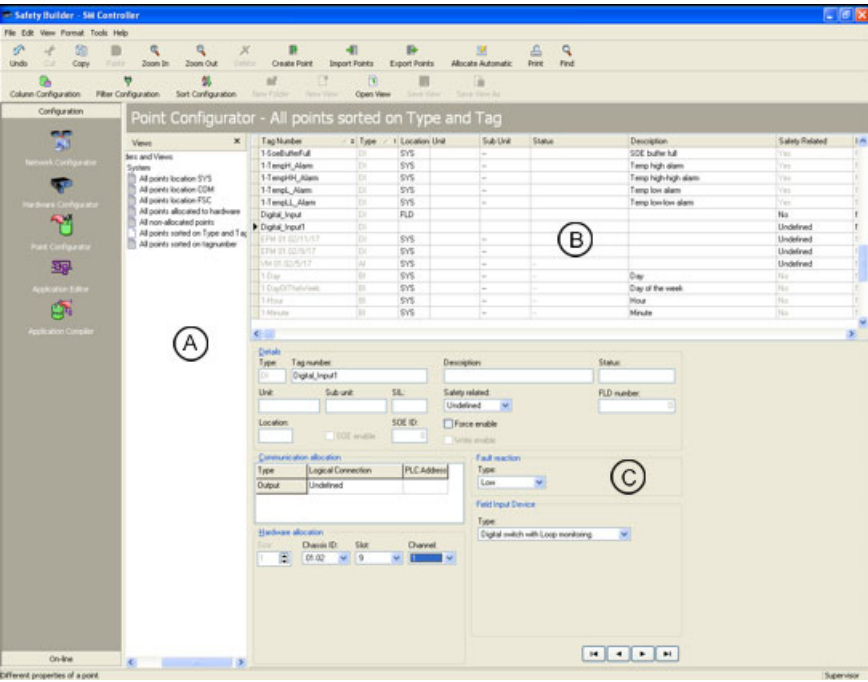


Note:

If you get a popup stating exclusive access is denied see “Working in a multi user environment” on page 143.

The Point Configurator main screen appears, which resembles Figure 16 on page 142.

Figure 16 Point Configurator main screen



This program window consists of the following sections:

- The menu bar, toolbars, outlook bar and status bar.
For a description of these bars see “Screen layout” on page 27.

a. Explorer bar

This section allows you to quickly change the View of the point database. You can use system Views (see “System Views” on page 149) or create custom Views (“Creating Views” on page 150).

b. Point database

The point database shows an overview of all points selected in the current View. You can configure the columns, filters and sort order (see “Configuring Views” on page 152).

c. Detailed View

You can select a point in the point database by clicking it. Its attributes will then be displayed in the detailed View. A detailed description of all point attributes can be found in “Allocating points” on page 160.

At the bottom of the detailed View you will find four navigation buttons



. You can use these buttons to navigate through the points in the point database.



Tip:

If you don't see the navigation buttons drag the split bar up.

The split bar is the bar that divides the point database area from the Detailed View area.

Working in a multi user environment



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
 2. To give up exclusive access to an SM Controller access the **Network Configurator**.
 3. To give up shared access exit the tool or function that demands shared access.
- To give up all access you can close the file (click **File>Close** from the menu bar).

When you try to access the SM Controller with multiple users simultaneously, access via this tool may be denied and you get a popup stating either:

Access is denied, please try again later.

Exclusive access is denied, please try again later.

- If the Plant database is opened for exclusive use by someone using Network Configurator, your access to this tool is denied.
- If the SM Controller database is opened by someone, using this or a similar tool, your access to this tool is denied.

In above cases, you cannot continue until the “denied access” lock is relieved by the other user(s).

For more information see also “Multi user environment” on page 36.

Point Configurator menu

Below list shows the Safety Builder Point Configurator menu structure.

The shortcut access key combinations, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also “Keyboard shortcut and access keys” on page 32.

| Menu item | Description |
|---------------------------------|---|
| <i>File</i> | |
| > C lose | Closes the Point Configurator. |
| > I mport <i>P</i> oints | Import points from an external database file. (See “Importing and exporting points” on page 162.) |
| > E xport <i>P</i> oints | Export points to an external database file format. (See “Importing and exporting points” on page 162.) |
| > P rint | Prints the current point configuration. For more information see “Print” on page 166. |
| > N ew f older | Create a new folder in the View bar (see “Working with Views” on page 148). |
| > N ew <i>V</i> iew | Creates a new View in the selected folder of the View bar (see “Working with Views” on page 148). |
| > O pen <i>V</i> iew | Opens the View selected in the View bar (see “Working with Views” on page 148). |
| > S ave <i>V</i> iew | Stores the configuration in the selected View (see “Working with Views” on page 148). |
| >Save <i>V</i> iew A s | Allows you to store the current View with a new name (see “Working with Views” on page 148). |
| > E xit | Exits Safety Builder. |

Edit

| | |
|-------------------------------------|--|
| >Undo | Undo the previous action. |
| >Cut | Cuts the value of the current cell. |
| >Copy | Copies the value of the current selection into copy-buffer. |
| >Paste | Paste the value of the copy-buffer into current cell. |
| >Delete | Deletes the value of the current cell. |
| >Select All | Selects all points in the point database. |
| >Create Point | Create a new point in the point database (see “Creating a point” on page 156). |
| >Allocate automatic | Allows you to allocate points automatically to hardware (see “Allocate automatic” on page 160). |
| >Find | Opens the Find dialog box and enables you to search for and replace text (see “Find Dialog” on page 164). |
| >Automatic communication allocation | Allows you to speed up the allocation process of the logical connections (see “Automatic communication allocation” on page 161). |

View

| | |
|-----------------------|--|
| >Toolbars | Toggles display of the toolbars. |
| >Outlook Bar | Toggles display of the Outlook bar. |
| >Audit Trail Viewer | Launches the Audit Trail Viewer (see “Audit Trail” on page 276). |
| >Views | Toggles display of the Views bar. |
| >Zoom in | Enlarge font size of point List. |
| >Zoom out | Reduce font size of point List. |
| >Auto fit | Scale to make all columns visible. |
| >Compilation Log File | Opens the Application Compiler log file. |

Format

| | |
|-----------------------|--------------------------------------|
| >Column configuration | View or change column configuration. |
| >Filter configuration | View or change filter configuration. |
| >Sort configuration | View or change sort configuration. |

| | |
|-------------------------------|---|
| Tools | |
| > C onfiguration | Displays a sub menu with available configuration tools. For an overview see “Safety Builder configuration tools” on page 41. |
| > O n-line | Displays a sub menu with available on-line tools. |
| > P assword | Launches the Security tool. |
| > O ptions | Enables you to set general program options. |
| Help | |
| > S afety Builder Help | Launches the Safety Builder Help function. |
| > A bout | Shows current version and license of the program. |

Toolbars



Note:

A toolbar only shows the most used tool functions and components. Some tool functions and components have to be accessed via an item in the Menu bar.

A toolbar contains a subset of tools or components that can be used by the active program.

Multiple toolbars can be active at the same time.

Configuration Dialog

The Configuration Dialog toolbar contains the components available to change the Views according to your requirements.

Click **View>toolbars>Configuration Dialog** to toggle the Configuration Dialog toolbar.

Point Configurator

The Point Configurator toolbar contains tools required to process points

Click **View>toolbars>Point Configurator** to toggle the Point Configurator toolbar.

Views bar

The Views bar is an Explorer bar as defined in “Explorer bar” on page 30. It allows you to quickly change the View of the point database.

For details see:

- “System Views” on page 149 and
- “Creating Views” on page 150

For information on views, see “Views” on page 147.

Using the Point Configurator

The Point Configurator gives direct access to the point database, in which you can view, print, create, configure or delete points and their attributes.

The Point Configurator uses views to realize this.

Before continuing, you should first familiarize yourselves with below topics:

| Topic | See |
|----------------------------------|----------|
| Point database | page 147 |
| Views | page 147 |
| Processing points | page 148 |
| Importing and exporting points | page 148 |
| Point Configurator shortcut keys | page 148 |

Point database

The point database contains system points, status points, diagnostic points and application points.

The point database contains the attributes for each point.

For details on what can be found in the point database, see “Point attributes” on page 391.

Views

You can access the point database by means of Views. Views allow you to filter the information in the point database, prompting you with relevant information only.

You can use (pre programmed) system Views or create your own Views.

For more on Views see “Working with Views” on page 148.

Processing points

By using a View, you can filter and select a single point or a group of points. These point can then be processed.

To work with points, see “Working with points” on page 156.

Importing and exporting points

You can import and export points, and point properties, to an external database to handle the process of creating and configuring points via an external application.

To import and export an external point database, see “Importing and exporting points” on page 162.

Point Configurator shortcut keys

Besides the shortcut keys listed in “Keyboard shortcut and access keys” on page 32, the following shortcut keys are active when you use the Point Configurator:

- **Ctrl+A** selects all points in the point database.
- **Ctrl+E** Toggles the display of the **Views bar**.
- **Ctrl+L** opens the **Configuration** window.
- **Ctrl+M** enlarges the font size of the point list.
- **Ctrl+O** reduces the font size of the point list.
- **Ctrl+N** opens the **Create Point** window.
- **Ctrl+T** opens the **Filter** window.
- **Ctrl+R** opens the **Sort** window.

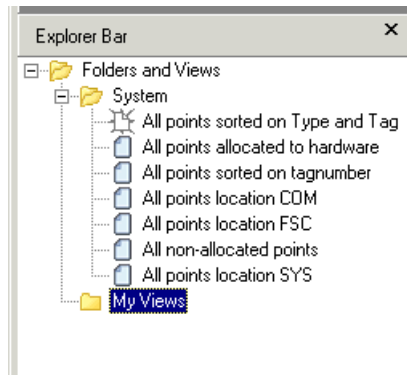
Working with Views

To simplify editing and viewing of points, the Point Configurator offers standard and custom Views. You can select a View to see only the points of your interest.

The standard Views available are listed in the Explorer bar (see Figure 17 on page 149 for an example). The standard Views are located in the **System** folder of the Explorer bar.

Figure 17 on page 149 displays the Point Configurator Explorer bar with a list of Views.

Figure 17 Point Configurator Views



System Views

Safety Builder Point Configurator is standard equipped with several system Views. Every View is located in the Explorer bar under the **System** folder.

You can activate a View by double-clicking it. The point database will then automatically switch to the selected View.

The following system Views are available:

- All points location SYS
- All non-allocated points
- All points sorted on tag number
- All points location COM
- All points sorted on Type and Tag
- All points location FSC
- All points allocated to hardware



Note:

- You cannot store new Views or delete Views in this System folder.
- You cannot save modified Views from the System folder. Use **Save as** instead and pick a different folder.

Switching Views

To switch Views, double-click the preferred View in the explorer bar.

Creating Views

Before creating a new View, you must set up and designate the folder in which the View will be stored. You cannot store custom Views in the system folder.

To store a new View, right-click **Folders and Views** in the explorer bar and select **New Folder**. Now enter a name for the folder.

In order to save the current View, click the **Save View As** button. A window appears, asking you to indicate the folder the View needs to be saved in (**Save Under Folder**) and to specify the name of the View (**Save As**).



Note:

Views must be added to custom folders. It is not possible to add Views to system folders.

Modifying Views

A number of Point Viewer elements can be customized:

- Configuration of columns
- Configuration of filters
- Configuration of the sort order

These configurations are described in “Configuring Views” on page 152.

You can also manually reorder the point view as described in “Sort Point View manually” on page 150.

Sort Point View manually

After you opened your View you may want to reorder the point listing manually.

- 1 To reorder the point listing in a View place your mouse cursor over the column you wish to reorder.
Figure 18 on page 151 shows that the cursor changes in a black arrow.
- 2 *Click once* to sort ascending (A to Z), *click twice* to sort descending (Z to A)
- 3 Select another column you want to sort on and repeat above step.
- 4 Repeat these steps until your sort is satisfactory.



Tips:

1. **To unselect** a column from sorting place the mouse cursor over the column and click once with the CTRL key pressed.
 2. If you want to save your sort configuration see “Sort configuration” on page 155.
-

Figure 18 The point listing 'All points located SYS' reordered

| r - All points location SYS | | | | | | |
|-----------------------------|-----------|----------|------|---------|--------|--|
| TagNumber | PointType | Location | Unit | SubUnit | Status | |
| Fault Reset SM Controller_2 | DO | SYS | | -- | | |
| Fault Reset SM Controller_3 | DO | SYS | | -- | | |
| SecSwitchOff | DO | SYS | | -- | | |
| Day | BI | SYS | | -- | -- | |
| DayOfTheWeek | BI | SYS | | -- | -- | |

The example in Figure 18 on page 151 shows a fraction of the View 'All points located SYS' reordered

- primarily descending by point Type,
- secondly ascending by Tag Number.

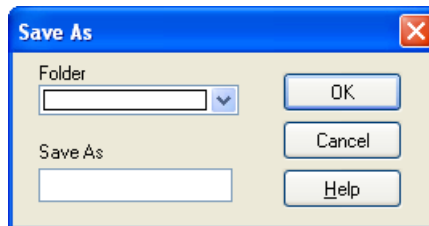
Saving Views

When you have made changes to a View or created a new View, you need to save it if you want to use it in the future.

If you want to override the current View with the changes you can select **File > Save View** from the menu. This option is not available for system Views.

If you want to store the View under a new name you can use **File > Save View As**. If you do so a window similar to Figure 19 on page 151 will appear: This option is available for system Views and custom Views.

Figure 19 Point Configurator Save As



Save Under Folder

Select the folder you want to save the View in. You must always select a folder.

If no folder for saving custom Views is present yet, you need to create a folder before you save the View. To create a folder, choose **File > New Folder** while selecting **Folders and Views** (or any previously made folder) in the Explorer Bar.

Save As

Enter the name you want to save the View under.

Configuring Views

In order to adjust the View according to your requirements, you can configure a number of display elements, which are described in this section.

Column configuration

To access this window, click the **Column Config** button in the toolbar or open it via the Format menu (**Format > Column Config**).

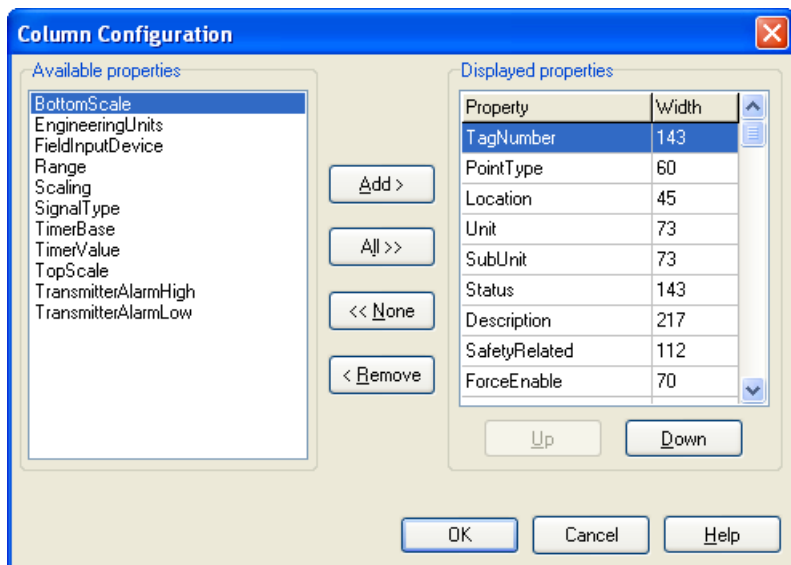
The window on the left shows the available properties that are currently not displayed in the selected View. The right-hand window shows the properties that are currently displayed. By moving properties from the **Available properties** column into the **Displayed properties** column or vice versa, you can indicate which point data you want the column to display.

The order of the items in the right-hand window represents the order of the selected items in the point database. The order can be changed by using the **up** and **down** buttons. You can also change the width of each column by modifying the **Width** value of the **Property**.



Tip:

A width always needs to be entered with three digits, so **10** should be entered as **010**.



| | |
|----------------------|---|
| Add > | Move the selected property Displayed properties . |
| All >> | Move all properties to Displayed properties . |
| << None | Remove all properties from Displayed properties . |
| < Remove | Remove the selected property from Displayed properties . |
| Up | Move the selected property up one level. |
| Down | Move the selected property down one level. |

Filter configuration

To access this window, click the **Filter Configuration** button in the toolbar or open it via the **Format** menu (**Format > Filter Configuration**).

In this window, you can filter points to View and hide selected points in the current View. By setting a number of criteria, you indicate which points you do want to be displayed and which point should not be displayed.

The screenshot shows a 'Filter Configuration' dialog box. It has a title bar with the text 'Filter Configuration' and a close button (X). The main area contains a 'Property' dropdown menu with 'TagNumber' selected, an 'Add' button, a 'Value' text input field, an 'Edit filter' button, and a 'Delete' button. Below these is a table with two columns: 'Property' and 'Value'. At the bottom are 'Filter', 'Cancel', and 'Help' buttons.

- Property** Sets the property you want to filter.
You can choose from all properties that are displayed in the selected View.
- Value** Sets the value of the property you want to filter.
The filter works case sensitive and the asterisk sign (“*”) can be used as a wildcard.
- Add** Adds the property and value to the filter list displayed in the bottom pane.
Adding a property and value means that only points where the added property has the added value are displayed.
For example: adding the property/value combinations “TagNumber=test*” and “Location=EXT” only displays points where the TagNumber starts with “test” and the Location equals “EXT”.
- Edit Filter** Edits the value or property from the selected item in the filter list.
- Update** Updates the value or property from the selected item in the filter list after you have edited it using the **Edit Filter** option.
- Delete** Deletes a filter from the filter list.
- Filter** Activates the filter with the displayed properties.

Sort configuration

**Tip:**

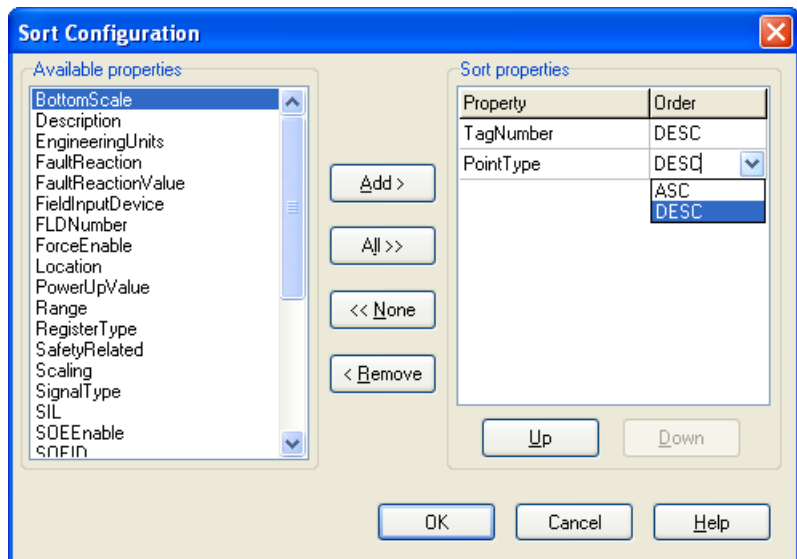
To manually change the order in which the points are sorted see “Sort Point View manually” on page 150.

To access this window, click the **Sort Configuration** button in the toolbar or open it via the **Format** menu (**Format > Sort Configuration**).

The **Sort configuration** settings determine the order in which points are displayed. The **Available properties** window on the left shows the available properties (shown in the **Displayed properties** list of the **Column configuration**). The **Sort properties** window on the right shows the priorities and the sorting order of points:

The top item in the **Sort properties** list will get the highest priority in the sorting order.

The sorting order can be set by clicking on **ACS** (ascending order) or **DESC** (descending order) in the **Order** column and choosing the correct order from the pull down menu. You can sort up to 16 items this way.



Add >

Add the selected property from **Available properties** to **Sort properties**.

All >>

Move all properties from **Available properties** to **Sort properties**.

| | |
|-----------------|--|
| << None | Remove all properties from Sort properties . |
| < Remove | Move the selected property from Sort properties . |
| Up | Move the selected property one level up. |
| Down | Move the selected property one level down. |

Working with points

This section contains information on creating and configuring points.

Point types


Table 4 on page 156 lists the point types available in Safety Manager.

Table 4 Safety Manager point types

| Type | Description | |
|------|----------------|---|
| DI | Digital input | Boolean input (either 0 or 1) |
| AI | Analog input | Input with type Long or Float [*] |
| BI | Binary input | Input with type Byte, Word, Long or Float [*] |
| DO | Digital output | Boolean output (either 0 or 1) |
| AO | Analog output | Output with type Long or Float [*] |
| BO | Binary output | Output with type Byte, Word, Long or Float [*] |
| M | Marker | Boolean |
| C | Counter | Word (range 0 - 8191) |
| T | Timer | Timebase ms, s, min |
| R | Register | Byte, Word, Long or Float [*] |

^{*} For an explanation of the register types (Byte, Word, Long, Float) see “Register type” on page 400.

Creating a point



Note:

When creating a new point, you must fill the type and tag number fields as these combined form a unique identifier for any point.

You can create points in the following ways:

1. Create a new point from the point database.
Right-click in the point database, and choose **Create Point**.

A pop-up menu opens, allowing you to choose the following point types: **DI**, **BI**, **AI**, **DO**, **BO**, **AO**. A new point of the selected type will be added to the point database.

2. Create a new point when editing an FLD.
This form of adding may also include points of other types, such as timers (T).
See “Application Editor” on page 178 for details.
3. Copy an existing point from the point database



Attention:

Tag name, description and allocation are unique identifiers for each point and cannot be copied. When copying a point, only the point type and the applied settings are copied.

- a. Click in the area directly left of the first column of the point you want to copy, so that all columns of this point are highlighted and an arrow appears left to the first column.
- b. Right-click in one of the fields of the selected point and choose **Copy**.
- c. Right-click anywhere in the point database and choose **Paste**.

A copy of the selected point will be added to the point database.

By selecting more than one point in the point database (by using shift-click) it is possible to copy and paste multiple points.

4. Copy an existing point from an FLD.
When copying (part of) an FLD with points allocated, the point types and applied settings are copied as well.
See “Application Editor” on page 178 for details.
5. Import an external point database containing new points.
See “Importing and exporting points” on page 162 for details.

Renaming a point



Note:

A download is not mandatory after renaming a point.

When you choose not to download after modifying tag numbers, the SM Controller will be unable to warn on-line users about the update involving modified tag numbers.

On-line users with a previous version of the application on their Safety Station will then be confronted with the old tag numbers.

User configurable points can be renamed, assuming no conflict consists with other points.

You can rename points in the following way:

- Double-click in the *TagNumber* field and edit the tag number
- Import an external point database containing a list of renamed points. For details see “Importing and exporting points” on page 162.

Deleting a point



Attention:

When you delete a point of type DI, BI, AI, DO, BO or AO from an FLD, the point is *not* removed from the point database.

On the other hand: logic symbols that are stored in the point database, such as timers (T) and registers (R) *are* removed from the point database when deleted from an FLD.

You can delete points in the following ways:

1. Click in the area directly left of the first column of the point you want to delete, so that all columns of this point are highlighted and an arrow appears left to the first column.
2. Right-click in one of the fields of the selected point and choose **Delete Point**. After a confirmation of the delete action, the selected point will be deleted. By selecting more than one point in the point database (by using shift-click) it is possible to delete multiple points.
3. Import an external point database containing a list of deleted points. For details see “Importing and exporting points” on page 162.

Points of types other than DI, BI, AI, DO, BO and AO, like timers (T), can only be deleted from the point database by deleting them from the FLD they are used in using the Application Editor (see “Application Editor” on page 178).

Configuring a point



Note:

Some attributes or properties of a point that are shown cannot be modified by the user.

When you configure a point you assign attributes to the point.

- Some attributes are filled by the user, others are filled by tools within Safety Builder.
- Note that a number of attributes are to provide information to the user; they are ignored by the system.

Configuration steps

point configuration can be split in the following steps:

1. **Creating a point**

In this initial step, you only fill the required parameters. For details, see “Creating a point” on page 156.

2. **Assigning primary properties to a point**

In this step you – or Safety Builder toolset – add the first set of properties to the point configuration.

Properties can be mandatory or descriptive.

- some provide information to a user and are ignored by the system,
- some are only visualized after the point has been allocated. (See step 4. on page 159.)

For more information see “Point properties” on page 167.

3. **Allocating points**

In this step you allocate a point to either hardware and/or communication channels. You can allocate points manually or automatically.

In addition you can allocate a number of communication devices you want to copy the point status to.

To learn how to allocate a point, see “Allocating points” on page 160.

4. **Finalizing properties**

Some properties relate to the allocation of a point and are therefore only visualized after allocation of that point. These properties are:

- a. **Fault reaction properties**

These apply to all allocated points. For details see “Fault Reaction” on page 173.

- b. **Analog specification**

Depending on the properties of the module an analog point is allocated on certain attributes may, or may not, apply to the configured analog point. For details see “Analog specification” on page 175.

- c. **Field input device**


Depending on the properties of the module a digital input point is allocated on certain attributes may, or may not, apply to the configured DI point. For details see “Field Input Device” on page 175.

Configuration procedure

You can configure or edit a point attribute in the following ways:

1. **Using predefined configuration views:**

- a. Right-click in the point database on the point you want to configure, and choose **Configure Point**.

- 2 A **Configure Point** window appears. In the upper part of this window, the setting and description fields of the selected point can be edited.
For details see “Point properties” on page 167.
 - a. Allocate the point to IO or a communication channel. For details see “Allocating points” on page 160.
 - b. Other points than the one currently selected can be configured by choosing a different combination of **Point type** and **Tag number**.
- 3 Using the embedded detail views:
 - a. Click in the point database on the point you want to configure
 - b. Edit the point attributes as they appear in the detail view below the point database. For details see “Point properties” on page 167.
 - c. Use the four navigation buttons  logical connection to navigate through the points in the point database.
- 4 Using fields directly in the point database:
It is possible to edit the properties of a point directly from the point database by clicking on the relevant property and changing it in the text box or pull down menu that appears. Obviously, this is only possible for properties that are displayed in the current View and are not shaded.
For details see “Point properties” on page 167.

Allocating points

You *must* allocate each point that is reflected in the application logic (FLD). To allocate a point the following steps are required:

1. allocate the point to
 - a. an IO module (see “Hardware allocation area” on page 172) or,
 - b. a communication device (see “Communication allocation area” on page 171 for details).
2. set the fault reaction of the point (see “Fault Reaction” on page 173),
3. optionally you can copy the point status to one or more communication devices (again see “Communication allocation area” on page 171 for details).

You will find the point configuration details at the bottom of the detail view, as shown in Figure 16 on page 142, or in a separate **Configure Point** window. For instructions how to access either one, see “Configuration procedure” on page 159.

Allocate automatic

All points can be allocated manually or automatically.

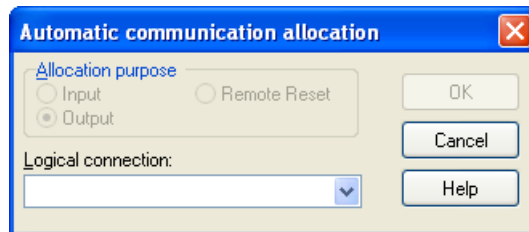
**Notes:**

1. Automatic allocation will function only when all points selected in the view are valid for allocation.
2. When allocating automatically, only the allocation fields are filled. Attributes such as SOE, Fault Reaction, etc. remain unchanged.
For an overview of the default settings see “Database field properties table” on page 412.)

- “Automatic communication allocation” on page 161 describes how to allocate points automatically to communication devices.
- “Automatic hardware allocation” on page 161 describes how to allocate points automatically to hardware.

Automatic communication allocation

To speed up the allocation process of the logical connections you can have this done automatically. To access this function select **Edit > Automatic communication allocation** in the menu.

**Allocation purpose**

Choose between

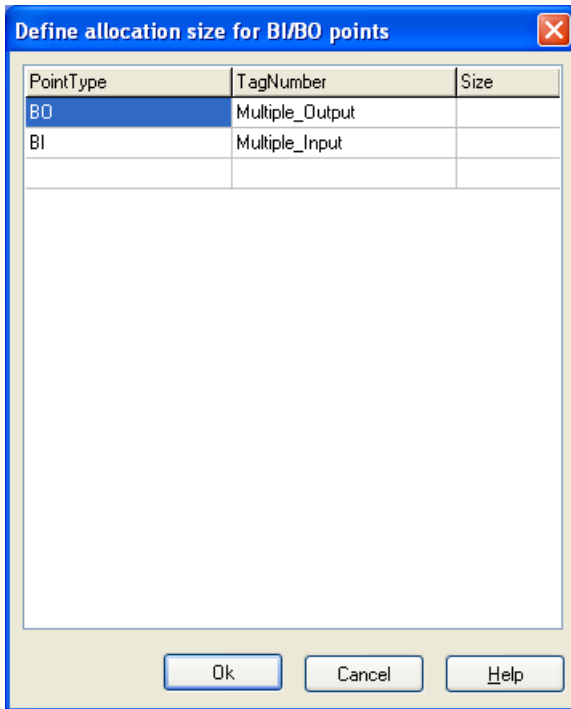
- **Input** (data entering the Controller)
- **Output** (data leaving the Controller) and

Logical connection

Choose which available logical connection is to be used.

Automatic hardware allocation

To allocate points automatically to hardware, select **Edit > Allocate Automatic** from the menu or choose the **Allocate Automatic** icon in the Toolbar.



Size

Here the user is requested to fill the number of allocated IO channels on an IO module to read or write *unsigned* binary values. The minimum size is 1, the maximum size is 31.

For more information see “Size” on page 402.

Allocate manually

All points can be allocated manually or automatically. When a point is manually allocated to hardware, you must assign a **Chassis**, **Slot** a **Channel** and a **Size** (if the point is of type BI or BO – for more information see “Size” on page 402.)

To allocate points manually you should:

- 1 Select a point from the point database.
- 2 Fill out the allocation details as described in “Point properties” on page 167.

Importing and exporting points

With the **Import Points** and **Export Points** functions you can import and export points from and to an external database application.

In the external application you can:

- **modify point properties** of multiple points by changing the exported point properties before re-importing the point database,
- **create multiple new points** by adding them to the exported point database before re-importing the point database,
- **rename multiple existing points** by listing the new name in the exported point database before re-importing the point database,
- **delete multiple existing points** by identifying them as such in the imported point database,
- **apply identical properties to new points** by copying existing points properties onto the new created points before re-importing the point database.

For information about import and export operations see:

- “Exporting point properties” on page 163
- “Importing point properties” on page 163

For information about external point database, its structure and operations see “Import and Export” on page 409.

Exporting point properties

To export Safety Manager point information select **File>Export Points**.

A popup window will appear to define the location and filename to save to.



Attention:

Make sure that the drive you are saving to has sufficient disk space.

Export will not warn if you run out of disk space. It is recommended to verify the content of the exported database after saving.

For detail information of the data exported, see “Import and Export” on page 409.

Importing point properties

To import Safety Manager point information select **File>Import Points**.

Select the file to import via the pop-up window and click **Open**.



Note:

1. When importing an unknown combination of tag number and point type, a new point is created to which the imported point properties will be applied.
 2. When importing a known combination of tag number and point type, the modified point properties will be applied, providing these properties can be applied.
 3. Point properties must be valid and comply to the application design rules as indicated in “Application design rules” on page 22 or the properties will be ignored.
-

During the import action a log file is created, logging the errors that may arise during the import action. For details see “Log file” on page 439.



Attention:

When errors are found during an import action, the faulty point properties will be ignored and default settings will be applied according the application design rules as indicated in “Application design rules” on page 22.

For detail information regarding the imported data, see “Import and Export” on page 409.

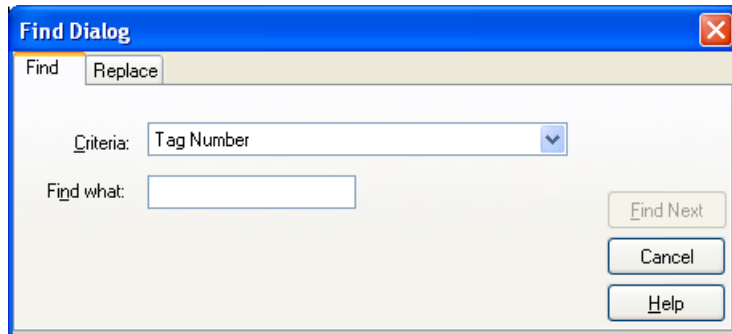
Find Dialog

You can use this function to search for specific points or change the value of an attribute you search for.

Find Dialog - Find tab

With this window you can find specific points.

You can access this window by clicking the **Find** button in the toolbar and then selecting the **Find** tab.

**Criteria**

Select which attribute you want to search in.

You can choose from:

- Point Type
- Tag Number
- Point Type & Tag Number
- Any string
- Enumerated Fields
- Not fully allocated

Find What:

The text or value to be searched.

Depending on the contents of **Criteria**, **Find What:** contains a drop down menu, a text field or a combination of both.

You can use an asterisk (“*”) as a wildcard. For example searching a tag number with “CP*”, will find all tag numbers that start with “CP”.

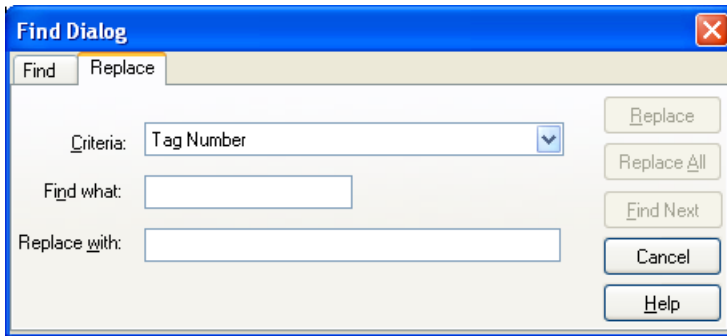
Find Next

Searches the next occurrence of the text in the **Find What** field.

Find Dialog - Replace tab

With this window you can find and replace specific points.

You can access this window by clicking the **Find** button in the toolbar and then selecting the **Replace** tab.

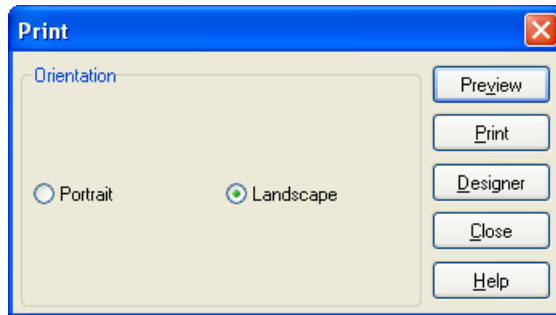


| | |
|---------------------|---|
| Criteria | Select which attribute you want to search in. You can choose from: <ul style="list-style-type: none">• Point Type• Tag Number• Point Type & Tag Number• Any string• Enumerated Fields• Not fully allocated |
| Find What | The text or value to be searched. Depending on the contents of Criteria, Find What: contains a drop down menu, a text field or a combination of both. You can use an asterisk (“*”) as a wildcard. For example searching a tag number with “CP*”, will find all tag numbers that start with “CP”. |
| Replace With | The text you want to use as a replacement |
| Replace | Replaces the selected instance. |
| Replace All | Replaces all occurrences of the search text. |
| Find Next | Searches the next occurrence of the text in the Find What field. |

Print

This windows allows you to print the listed point configuration.

To access select **File > Print** from the menu.



| | |
|--------------------------------|--|
| Portrait (orientation) | The report will be printed in a portrait orientation. This option is only available for a Columnar Report. |
| Landscape (orientation) | The report will be printed in a landscape orientation. This option is only available for a Columnar Report. |
| Preview | Shows a preview of the selected report. |
| Print | Prints the selected report. |
| Designer | Opens the report design utility. For more information on using this utility, see the user manual for FastReport (version 2.5). |
| Close | Close the print dialog without printing. |
| Help | Launches the Safety Builder Help function. |

Point properties



Tip:

For an overview of all point related attributes, see “Point attributes” on page 391.

This topic discusses the different point properties available via:

- the Point Configurator tool,
- the **import/export** function.

For the ease of discussion we based this topic on the assumption that you use Point Configurator to access the point properties.

“Importing and exporting points” on page 162 explains how you can address the same properties via the **import/export** function.

Figure 20 Typical point properties window

The screenshot shows the 'Point Properties' dialog box with the following sections and callouts:

- 1** Point type: AI, Tag number: Analog_Input
- 2** Details: Type: AI, Tag number: Analog_Input, Description: (empty), Unit: (empty), Sub unit: (empty), SIL: (empty), Safety related: Undefined, FLD number: 0, Location: (empty), SOE ID: 0, Force enable (unchecked), Write enable (unchecked)
- 3** Communication allocation: Table with columns Type, Logical Connection, PLC Address. Row 1: Output, Undefined, (empty).
- 4** Hardware allocation: Size: 1, Chassis ID: (empty), Slot: (empty), Channel: (empty)
- 5** Fault reaction: Type: Bottom scale
- 6** Analog specification: Signal type: 4-20mA, Scaling (checked), Bottom scale: 0, Top scale: 0, Engineering units: (empty), Transmitter alarm: Low 3, High 20.93, SOE Setpoint: Low --, High --

Buttons at the bottom: OK, Cancel, Apply, Help

Figure 20 on page 168 shows a typical point properties window that is accessible via Point Configurator. This window can be divided in several areas, each of which are discussed in more detail:

1. This area is used to select the point you want to view/edit.
For more information, see “Point selection area” on page 169.
2. Here you can view/edit the main properties of a point.
For more information, see “Point details area” on page 169.
3. This area is to view/edit the communication allocation of a point.
For more information, see “Communication allocation area” on page 171.
4. This is were you define the hardware allocation of a point.
For more information, see “Hardware allocation area” on page 172.

5. Here you define the fault reaction of an allocated point.
For more information see “Fault Reaction” on page 173.
6. Some points require extra specifications. These are located in this area.
For more information, see “Point specific detail area” on page 174.

Point selection area



Tip:

In this area you select existing points, you cannot create new points here.

- To manually create a new point see “Creating a point” on page 156.
- To import a new point see “Importing point properties” on page 163.

This area in the point properties window lets you select the point you want to view/modify.

Point type

Use this pull down box to select an existing point type.

A description of available point types can be found in “Point Type” on page 393.

Tag number

Use this pull down box to select an existing tag number matching the point type.

Point details area

This area in the point properties window lets you define the main point properties.



Note:

Following display detail is an example containing all optional fields.

It does not exist as such.

| | |
|-----------------------|--|
| Type | This “view only” field displays the selected point type. A list of available point types can be found in “Point Type” on page 393. |
| Tag number | Use this text field to view/modify the tag number of the point. For more details see “Tag number” on page 394. |
| Description | Use this text field to view/modify the point description. For more details see “Description” on page 394. |
| Status | This field is only visible for digital points. Use this text field to view/modify the point status description. For more details see “Status” on page 394. |
| Unit | Use this text field to view/modify the field unit the point is located in. For more details see “Unit” on page 395. |
| Subunit | Use this text field to view/modify the field subunit the point is located in. For more details see “Subunit” on page 395. |
| SIL | Use this text field to view/modify the SIL level of the point. For more details see “SIL” on page 395. |
| Safety related | Use this text field to view/modify the listed safety relation of the point. For more details see “Safety related” on page 396. |
| Power up | This field is not visible for inputs allocated on hardware. Use this field to view/modify the power up value of the point. For more details see “Power up” on page 399. |
| FLD Number | This field identifies the FLD the point is used on. If the point is not used on any FLD its value is 0. |
| Location | Use this text field to view/modify the location of the point. For more details see “Location” on page 394. |
| SOE Enable | Use this check box to enable sequence of events on the point. For more details see “SOE Enable” on page 397. |
| SOE ID | This field shows the assigned SOE ID if <i>SOE enable</i> or <i>Force enable</i> is checked <i>and</i> SOE collection on the SM Controller is enabled. Use this field to view the SOE ID of the point. For more details see “SOE ID” on page 397. |
| Force Enable | Use this check box to enable forcing on the point. For more details see “Force enable” on page 398. |

Write Enable

This check box is only available for input points with location COM.

Use this check box to enable writing of the point. For more details see “Force enable” on page 398.

Register type

This field is only displayed in combination with binary points and identifies the format of the point data.

Note:

This field cannot be modified if the binary point is allocated on hardware. To modify see “Hardware allocation area” on page 172 instead.

For available register types see “Register type” on page 400.

Communication allocation area



Tip:

For more information see “Communication allocation” on page 403.

This area in the point properties window lets you define the communication allocations of points.



Notes:

1. If the point is an input with location COM or FSC the communication allocation area contains an **input allocation**.
 2. For each point you can assign multiple **output allocations**, one for each created logical connection.
-

Communication allocation

| Type | Logical connection | PLC address |
|--------|-------------------------------|-------------|
| Input | Experion Server-SM Controller | 10001 |
| Output | Undefined | |

Undefined

Safety Builder-SM Controller_1

DCS-SM Controller_1

SM Controller_1-SM Controller_2

SM Controller_1-SM Controller_3

- Allocation** This column defines the type of communication allocation.
- By assigning the **Output** type to a point (any point) you allow it to be monitored by the allocated communication device. A point can be allocated as an output to multiple logical connections simultaneously.
 - An input point can be written by the allocated communication device that has the **Input** type assigned. You can only assign the **Input** type once on input points with location COM or FSC.
- For more details see “Point details area” on page 169.

Logical connection This column contains pull-down boxes that define the logical connection per input/output allocation. The choice of options is determined by the configured logical connections.

To open you must double click the pull-down box.


For more information see “Creating a logical network” on page 52.

PLC address This column defines the allocation of this point on the logical connection.

To alter you must double click the pull-down box.

For more information see “PLC address” on page 405.

Hardware allocation area



Notes:

This area is not shown when the point has location COM.

This area in the point properties window lets you define the hardware allocation of the specified point properties.

Size

Lets you define the number of bits of a binary point to be allocated on the hardware. For more information see “Size” on page 402.

- Safety Builder automatically changes the **Register type** to match the number of allocated bits. See “Point details area” on page 169 for more details.

Chassis

Identifies the chassis containing the IO module.

For more information see “Chassis” on page 403.

Slot

Identifies the slot ID of the IO module.

For more information see “Slot” on page 403.

Channel

Identifies the IO channel the point is allocated on.

For more information see “Channel” on page 403.

Fault Reaction

**Attention:**

Assuming the point allocation hardware/protocols support the chosen fault reaction, you can set the fault reaction on a *per channel basis*, with the exception of DO.

- **A DO fault reaction setting is implemented on output module level:**
If you change/set the fault reaction setting of one DO channel, you therewith change the setting of *all* DO channels on that output module.

When you allocate a point, the specific detail area is used to specify the fault reaction on that point.

The attributes you can enter depends on the type of signal and the allocation:

Table 5 on page 173 shows the possible fault reaction settings for hardware IO.

Table 5 Fault Reaction settings for hardware IO

| Signal type | Fault Reaction settings |
|----------------|-------------------------|
| Digital Inputs | High/Low/Scan/Hold |

Table 5 Fault Reaction settings for hardware IO

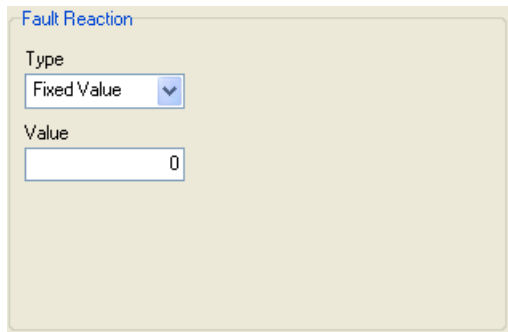
| Signal type | Fault Reaction settings |
|-----------------|----------------------------------|
| Digital Outputs | Low/Appl |
| Analog Inputs | Top Scale/Bottom Scale/Scan/Hold |
| Analog Outputs | 0 mA/Appl |

Table 6 on page 174 shows the possible fault reaction settings for communication IO.

Table 6 Fault Reaction settings for communication IO

| Signal type | Fault Reaction settings |
|---|-------------------------|
| Digital Points (DI) | High/Low/Freeze |
| Numeric Points (BI) (The default fixed value for numerics is 0.) | Fixed Value/Freeze |

For an overview and understanding of the fault attributes reaction and what this means see the *Overview Guide*.



- Type

This field defines the fault response for this particular point.
Applicable attributes to this field are listed in Table 5 on page 173 and in Table 6 on page 174.
- Value

This field contains the fixed value of the point, in case Fixed Value was chosen as fault reaction type.

Point specific detail area

This area contains point specific items. Which details are displayed here depends on the point type and the allocation of the point.

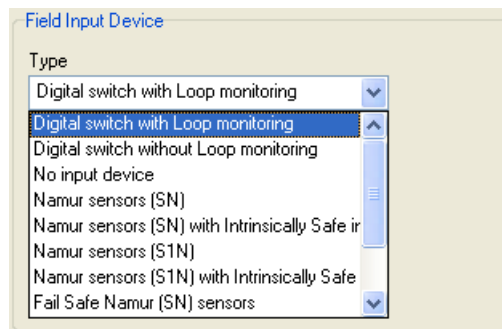
Field Input Device

Note:

This field is only visible when input modules are selected that support the listed options.

When you allocate an input on a special purpose input module, such as a line monitored digital input module type SDIL-1608, the point specific detail area is used to specify the type of field device.

This information allows the system to correctly interpret the signal from that device.



Type

With this field you identify the type of sensor connected to the physical channel.

For an overview of available options and their interpretation see the data sheet of the chosen input module. You can access such a data sheet via the *Hardware Reference*.

Analog specification



Tip:

For more information related to analog signal specifications see “Detailed attributes” on page 396.

When you open or create an analog point the point specific detail area is used to define the analog specifications on that signal.

Analog specification

| | | | |
|--------------------|-------------------|-------------------|---|
| Signal Type | <div>4-20mA</div> | | <input checked="" type="checkbox"/> Scaling |
| Bottom scale | <div>655</div> | Top scale | <div>3276</div> |
| | | Engineering units | <div></div> |
| Transmitter Alarm: | Low | High | |
| | <div>3</div> | <div>20.93</div> | |
| SOE Setpoint: | Low | High | |
| | <div>655</div> | <div>655</div> | |

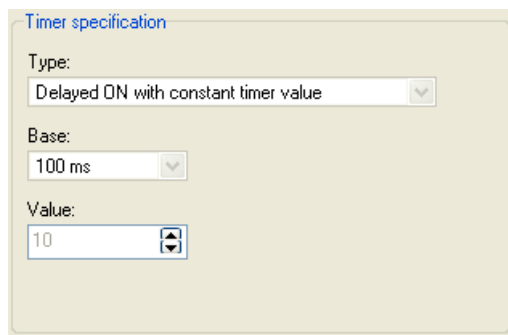
| | |
|-------------------|--|
| Signal Type | Use this field to define the type of signal being used by the analog channel. The available options depend on the selected analog IO module for the point. For details see the corresponding data sheet in the <i>Hardware Reference</i> . |
| Scaling | This check box determines if the field signal is scaled or not: <ul style="list-style-type: none">• When checked the field signal is converted into engineering units before being read by the application.• When unchecked RAW counts are used (with 0 being no signal, 3276 top scale (100%) and 4095 being full scale) If Scaling is checked, then both Bottom scale , Top scale and Engineering units must be entered. |
| Bottom scale | Represents the scale corresponding with the valid bottom value of the field signal: <ul style="list-style-type: none">• 0 or 655 for unscaled signals• user definable for scaled signals |
| Top scale | Represents the scale corresponding with the valid top value of the field signal: <ul style="list-style-type: none">• 3276 for unscaled signals• user definable for scaled signals |
| Engineering units | Specifies the engineering units when scaling is checked. |
| Transmitter Alarm | The Low and High transmitter alarm values define the values at which a sensor out of range (SensAI) alarm is raised by the system. By defining 0 or 25 you deactivate the transmitter alarm. |
| SOE Setpoint | The Low and High SOE Setpoint values define the values at which a sequence of event message is generated by the SM Controller. |

Timer Specification

Note:

This field is only visible when the selected item is a timer.

When you select a timer from the point database, the point specific detail area is used to *show* the timer properties: To change you must access the timer properties via the Application Editor.



Timer specification

Type:
Delayed ON with constant timer value

Base:
100 ms

Value:
10

Type

This field shows the type of timer applied. The type identifies the timers' response when triggered.

For an overview of timer types see "Timers" on page 371.

Base

This field shows the smallest unit of a time period.

Value

This field identifies the number of base units the timer will be active.

For more information see "Time functions details" on page 375.

Application Editor

The Application Editor tool enables you to create Functional Logic Diagrams (FLDs). Functional Logic Diagrams are combinations of logical operators that connect input signals to output signals.

When these diagrams are compiled, a Safety Manager executes them one by one in the sequence of the sheet numbers (from the lowest sheet number to the highest). Because of this execution sequence, you must take the following issues into account when drawing FLDs:

- Draw the input circuits first, then the logic and finally the output circuits.
- Prevent loop-back references as much as possible.

This section covers the following topics:

| Topic | See |
|---------------------------------|----------|
| Starting the Application Editor | page 178 |
| Application Editor Menu | page 180 |
| Toolbars | page 182 |
| FLD's bar | page 183 |
| FLD layout | page 183 |
| Using the Application Editor | page 185 |
| FLD types | page 187 |
| Handling FLDs | page 189 |
| Adding logic symbols | page 200 |
| Drawing logic | page 216 |
| Creating Revisions | page 219 |
| Finding points | page 220 |
| Printing | page 221 |

Starting the Application Editor

To start the Application Editor:

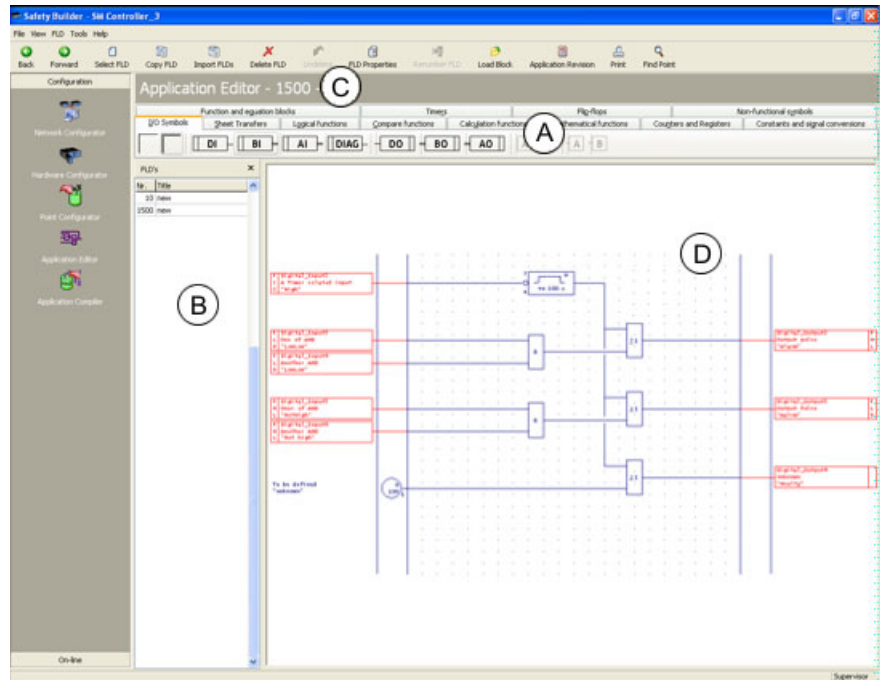
- Click the Application Editor icon in the **Outlook bar**,
- click **Tools > Configuration > Application Editor** on the **Menu bar** or,
- press the shortcut keys **Alt, T, C, A**

**Note:**

If you get a popup stating exclusive access is denied see “Working in a multi user environment” on page 181.

The Application Editor screen appears, which resembles Figure 21 on page 179.

Figure 21 Application Editor screen



The workarea of the Application Editor contains the following panes:

- Symbol library for creation of FLDs.
- Overview of available FLDs of current Controller. You can select an FLD by double clicking it in this list.
- Title of current FLD.
- Drawing area of selected FLD.

Application Editor Menu

Below list shows the Safety Builder Application Editor menu structure.

The shortcut access key combinations, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also “Keyboard shortcut and access keys” on page 32.

| Menu item | Description |
|--|---|
| <i>File</i> | |
| > C lose | Closes the Application Editor. |
| > P rint | Activates the print dialog (see “Creating Revisions” on page 219). |
| > E xit | Exits Safety Builder. |
| <i>View</i> | |
| > T oolbars | Toggles display of the toolbars (“Application Editor” and “Go to” toolbars). |
| > O utlook bar | Toggles display of the Outlook bar. |
| > A udit Trail Viewer | Launches the Audit Trail Viewer (see “Audit Trail” on page 276). |
| > F LD’s | Toggles display of the FLD list. |
| > S caling | Opens the scaling window where you can choose how to scale the FLD drawing area. Note that this scaling does not have an effect until the next time you start the Application Editor. |
| > C ompilation Log <i>File</i> | Opens the Application Compiler log file. |
| <i>FLD</i> | |
| > N ew FLD | Creates a new FLD (see “Creating a new FLD” on page 190). |
| > C opy FLD | Copies an FLD (see “Copying an FLD” on page 191). |
| > I mport FLDs | A wizard to import or duplicate multiple FLDs (see “Importing FLDs” on page 195). |
| > D elete FLD | Removes selected FLD (see “Deleting an FLD” on page 192). |
| > F LD Properties | Views or changes properties of selected FLD (see “FLD properties” on page 193). |
| > R enumber FLD | Renumbers an FLD (see “Renumbering FLDs” on page 193). |

| | |
|-------------------------------|---|
| > <i>Load Block</i> | Loads a previously saved part of an FLD into the current FLD (see “Saving and loading blocks” on page 218). |
| > <i>Application revision</i> | Shows revisions of selected FLD (see “Creating Revisions” on page 219). |
| > <i>Find Point</i> | Searches on which FLD a point is used (see “Finding points” on page 220). |
| > <i>Last Symbol</i> | Adds a symbol to the FLD, identical to the last selected symbol. |
| Tools | |
| > <i>Configuration</i> | Displays a sub menu with available configuration tools. For an overview see “Safety Builder configuration tools” on page 41. |
| > <i>On-line</i> | Displays a sub menu with available on-line tools. |
| > <i>Password</i> | Launches the Security tool (see “Entering password” on page 282). |
| > <i>Options</i> | Enables you to set general program options (see “Options” on page 274). |
| Help | |
| > <i>Safety Builder help</i> | Launches the Safety Builder Help function. |
| > <i>About</i> | Shows current version and license of the program. |

Working in a multi user environment



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
 2. To give up exclusive access to an SM Controller access the **Network Configurator**.
 3. To give up shared access exit the tool or function that demands shared access.
- To give up all access you can close the file (click **File>Close** from the menu bar).

When you try to access the SM Controller with multiple users simultaneously, access via this tool may be denied and you get a popup stating either:

Access is denied, please try again later.

Exclusive access is denied, please try again later.

- If the Plant database is opened for exclusive use by someone using Network Configurator, your access to this tool is denied.

- If the SM Controller database is opened by someone, using this or a similar tool, your access to this tool is denied.

In above cases, you cannot continue until the “denied access” lock is relieved by the other user(s).

For more information see also “Multi user environment” on page 36.

Toolbars



Note:

A toolbar only shows the most used tool functions and components. Some tool functions and components have to be accessed via an item in the Menu bar.

A toolbar contains a subset of tools or components that can be used by the active program.

Multiple toolbars can be active at the same time.

Application Editor toolbar

The Application Editor toolbar contains the following buttons:

| | |
|-----------------------------|---|
| Back | Browses to the previous FLD. |
| Forward | Browses to the next FLD. |
| Select FLD | Lets you select or create an FLD (see “Creating a new FLD” on page 190). |
| Copy FLD | Copies an FLD (see “Copying an FLD” on page 191). |
| Import FLD | Lets you import multiple FLDs (See “Importing FLDs” on page 195). |
| Delete FLD | Removes selected FLD (see “Deleting an FLD” on page 192). |
| Undelete | Undoes the latest Delete action. |
| FLD Properties | Views or changes properties of selected FLD (see “FLD properties” on page 193). |
| Renumber FLD | Renumbers an FLD (see “Renumbering FLDs” on page 193). |
| Load block | Loads a previously saved part of an FLD into the current FLD (see “Saving and loading blocks” on page 218). |
| Application revision | Shows revisions of selected FLD (see “Creating Revisions” on page 219). |

| | |
|-------------------|---|
| Print | Activates the print dialog (see “Creating Revisions” on page 219). |
| Find Point | Searches on which FLD a point is used (see “Finding points” on page 220). |

FLD's bar

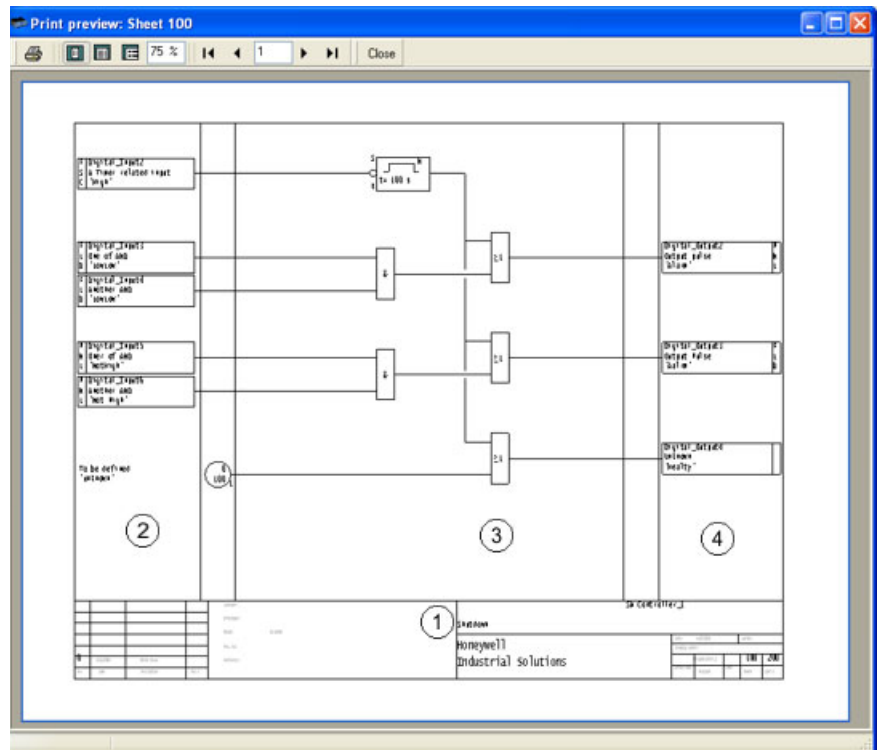
The **FLD's bar** is an Explorer bar as defined in “Explorer bar” on page 30. The **FLD's bar** provides an overview of available FLDs of current Controller.

You can select an FLD by double clicking it in the **FLD's bar**.

FLD layout

Figure 22 on page 183 shows an example of an FLD, which consists of the following areas:

Figure 22 FLD layout (hardcopy)



1. Information area (bottom)
2. Input area (left)
3. Control function area (center)
4. Output area (right)

Input area

The input area on the left side of the FLD contains all the inputs of the FLD. Inputs either originate from field equipment or other systems.

You can use values from other FLDs with sheet transfer functions. This enables the design of complex functions across multiple FLDs.

Control function area

The control function area in the center of the FLD contains the logic of the FLD. The function is realized by placing symbols and making connections between them. There is a variety of symbols which include among others logical, numerical, and time-related functions. In addition to these predefined symbols, the FLDs also support user-definable blocks:

- Function blocks

A function block is an FLD that can be used as a symbol in other FLDs. In this way you draw the logic only once and use it many times.

- A function block FLD must have a higher number than the control blocks used for the regular logic.
- A function block FLD must have a FLD number of 500 or above

You refer to a function block by its sheet number. A function block has inputs and outputs to transfer values but it does not support system outputs and off-sheet references.

- Equation blocks

An equation block is an FLD that can be used as a symbol in other FLDs and contains a tabular definition of a complex function such as a non-linear equations.

- A equation block FLD must have a higher number than the control blocks used for the regular logic.
- A equation block FLD must have a FLD number of 500 or above

You refer to an equation block by its sheet number. An equation block has a binary input and output to transfer floating point values.

Output area

The output area on the right side of the FLD contains all the outputs of the FLD. Outputs either drive field equipment or are transferred to other systems.

Information area

The information area at the bottom of the FLD contains the identification and revision details of the FLD. This section is only shown when the FLD is printed.

Using the Application Editor

You use the Application Editor to create or modify the application of Safety Manager.

An application is quickly created or modified by drawing logic using IEC 61131-3 compliant symbols and connections. The logic is stored on so-called Functional Logic Diagrams (FLDs).



Attention:

When you create logic, it is important to consider:

1. The compiler compiles the logic from the highest FLD number backwards.
 2. Function blocks and equation blocks must have a higher number than the FLDs to be created.
 3. Nested function blocks have a higher number than the function block that references them.
-

This section covers the following topics:

| Topic | See |
|----------------------|----------|
| FLD types | page 187 |
| Handling FLDs | page 189 |
| Adding logic symbols | page 200 |
| Drawing logic | page 216 |
| Creating Revisions | page 219 |
| Finding points | page 220 |
| Printing | page 221 |

Application Editor shortcut keys

The following shortcut keys are active when drawing with the Application Editor:

- press **PageUp** or **PageDown** key on your keyboard to scroll one FLD up or down.
- press **S** to select and draw a single line
- press **D** to select and draw a double line
- press **L** to select and draw the last selected symbol
- press **CTRL+B** to load a block (for details see “Saving and loading blocks” on page 218)
- press **CTRL+S** to select an FLD or create a new FLD.

When you *right-click* a symbol in an FLD you can:

- press **C** to copy the symbol
- press **D** to delete the symbol
- press **R** to drag the symbol
- press **M** to move the symbol
- press **H** to change the symbol
- press **P** to open the properties of the symbol

For general information on shortcut keys see “Keyboard shortcut and access keys” on page 32.

For details on drawing lines and other symbols see “Drawing logic” on page 216.

Scaling



Tip:

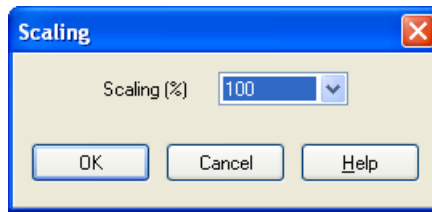
It is advised to scale the FLD such that it fits the work area without having to use any scroll bars.

Depending on the screen resolution set on your Safety Station and after toggling the FLD's bar of the Application Editor on or off, you might want to optimize the scale of the FLD.

You can open the **Scaling** window by clicking **View>Scaling**.

You must exit and restart Safety Builder for the scaling to take effect.

Figure 23 Scaling FLDs



FLD types

FLDs can be configured to contain other information than just application logic. You can define the FLD type via the **FLD Properties** window, as described in “FLD properties” on page 193.

Comment block

This is an FLD type that contains descriptive texts and/or symbols which are not placed in the variable database (e.g. cover sheet, legend of symbols).

Comment blocks are ignored by the Application Compiler.

FLD index

This type of FLD contains no logics, but is only used for printing FLDs. It is used to generate an index of all FLDs used in the application and is automatically updated by the Application Editor.

FLD index blocks are only visible when printing FLDs. FLD index blocks are ignored by the Application Compiler.

Tagnumber index

This type of FLD contains no logics, but is only used for printing FLDs. It is used to generate an index of all IO tag numbers used in the application and is automatically updated by the Application Editor.

Tag number index blocks are only visible when printing FLDs. Tag number index blocks are ignored by the Application Compiler.

Program block

This is the default FLD type and contains the main application logic.

You can view a program block by selecting its FLD number in the FLD's Bar.

Function block

This is an FLD type which contains a specific application function that can be called from other FLDs (program blocks or other function blocks). *Only FLDs with an Sheet number of 500 or higher can be defined as Function block.*



Attention:

In some occasions changes to the function block input and output *properties* are not automatically updated on the FLDs that call the function block.

For details see “Function block” on page 367.

You can open existing function blocks by selecting its FLD number in the FLD’s Bar or by double clicking a function block in an open FLD.

Equation block

This is an FLD type which contains an equation approximation based on interpolation,. Equation blocks can be used in other functional logic diagrams to approximate equations. *Only FLDs with an Sheet number of 500 or higher can be defined as Equation block.*

To view the equation approximation table:

- 1 select its FLD number in the **FLD’s bar**
- 2 Open the **FLD properties** and click the **View file** button
- 3 The **Equation file** popup window will open.

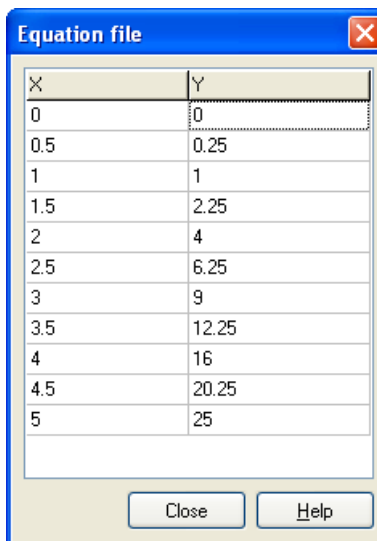
Equation file

The **Equation file** popup window, as shown in Figure 24 on page 189 displays the equation file contained within the equation block. This window has view functionality only.

To open the **Equation file** window open the **FLD properties** and click the **View file** button.

To modify the equation file you must import a new equation table. For more information about creating and importing equation tables see “Creating equation blocks” on page 210.

Figure 24 Equation file table



The screenshot shows a dialog box titled "Equation file" with a standard Windows-style title bar (blue with a close button). Inside the dialog is a table with two columns, "X" and "Y". The table contains 11 rows of data. Below the table are two buttons: "Close" and "Help".

| X | Y |
|-----|-------|
| 0 | 0 |
| 0.5 | 0.25 |
| 1 | 1 |
| 1.5 | 2.25 |
| 2 | 4 |
| 2.5 | 6.25 |
| 3 | 9 |
| 3.5 | 12.25 |
| 4 | 16 |
| 4.5 | 20.25 |
| 5 | 25 |

Handling FLDs

Opening an FLD

When you start the Application Editor, the first FLD of the selected Safety Manager is automatically displayed in the design screen, if available. To open another FLD, double-click its name or number in the FLD list.

When you open another FLD, the current FLD is automatically saved.

Navigating through FLDs

Several options are available to navigate through FLDs once you have an FLD open.

If you:

- press the **PageUp** or **PageDown** key on your keyboard you will scroll one FLD up or down.
- double-click an onsheet or offsheet reference in an FLD you jump to the FLD that the sheet reference points to.
- double-click a Function Block in an FLD you jump to the Function Block FLD.
- use the **Find Point** option you jump to the FLD the point is used on.

- double-click another FLD in the **FLD bar**, that FLD will open.
- click the **Back** or **Forward** button in the **Go to** toolbar you can browse the history of viewed FLDs.

Creating a new FLD

To create an FLD, choose **FLD > Select FLD** and type a new FLD number.

Figure 25 Creating a new FLD

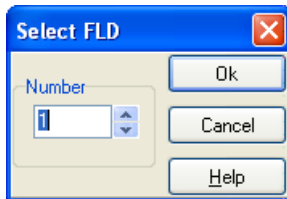


Figure 25 on page 190 shows that you will be asked for the number of the new FLD, followed by the properties of the new FLD.

For more information see:

- “FLD properties” on page 193 and
- “Nesting FLDs” on page 195

Editing an FLD



Attention:

When you change, redraw, disconnect, relocate existing logic on FLDs or import entire FLDs, the embedded compiler markers and registers may be removed or regenerated, thus affecting the actual field states during an OLM.

Note that renumbering FLDs does not affect the field states during an OLM.

During an OLM the following should be considered:

- **All new or regenerated points on a modified FLD start with their power-up value.** This includes all regenerated compiler markers and registers and all imported and copied logic.



Note:

For detailed rules on modifying live FLDs, see the *On-line Modification Guide*.

If you edit an FLD, you should consider the effect of loading the modified FLD online in a live system (if applicable).

When editing an FLD see:

- “FLD properties” on page 193
- “Adding logic symbols” on page 200
- “Drawing logic” on page 216
- “Creating Revisions” on page 219 and
- “Compiler registers and markers” on page 233.

Copying an FLD

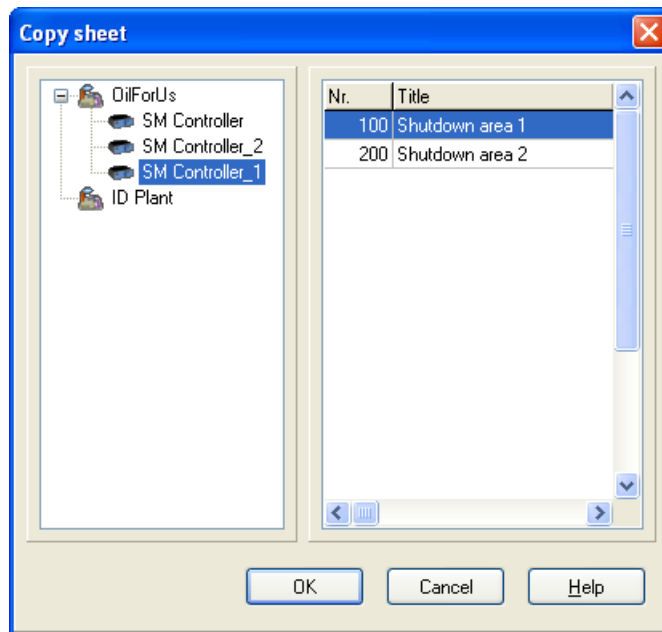


Tip:

If you want to copy multiple FLDs it is easier to use the **Import FLD** wizard as described in “Importing FLDs” on page 195.

The function **FLD > Copy FLD** imports all elements from an FLD into the current FLD. When you want to create an FLD that is similar to an existing FLD you can use this copy function.

To open the **Copy Sheet** window choose **FLD > Copy FLD**. The following window will appear:



The left window displays a tree view of the controllers in the currently selected plant. You must select the controller that contains the FLD you want to copy.

The right window displays a list of FLDs that is present in the selected controller. Here you select the FLD you want to copy.

Clicking **OK** will import all elements from the selected FLD into the current FLD.

To make a copy of an existing FLD, do the following:

- 1 Make a new FLD by using the option **FLD > New FLD**.
- 2 Import all elements from the FLD you want to make a copy of into the new FLD by using the **FLD > Copy FLD** option.

Deleting an FLD



Attention:

Equation blocks cannot be deleted as normal FLD's. There are two ways to delete an equation block:

- import an empty equation table in the equation block
- Change the block type to a Comment block, click **OK** and delete the FLD.

To delete an FLD, choose **FLD > Delete FLD**.

After a confirmation, this will remove all blocks from the current FLD, but will leave the FLD listed in the FLD list for now. At this moment, the delete action can be undone by clicking the **Undelete** button.

When you double-click another FLD in the FLD list, the deleted FLD is removed from the FLD list.

Renumbering FLDs



Note:

You can only renumber an FLD when *Online modification* option in the **SM Controller properties** is set to NO.

You can change the number of an FLD by choosing **FLD > Renumber FLD**. A window will appear, asking you for the new number of the FLD.

FLD properties

In the **FLD Properties** window, you can edit the properties of the selected FLD and define the FLD block type.

The FLD Properties window also contains:

- A **Revisions** sub window, in which you can view the revision data of the selected FLD. For more information, see “Update the revision ID of a single FLD” on page 220.
- A **View file** sub window, in which you can see the contents of an equation block.

To open the FLD Properties window, choose **FLD > FLD Properties**.

The image shows a 'Properties' dialog box with a blue title bar and a close button (X) in the top right corner. The dialog is divided into two main sections. The left section, titled 'FLD properties', contains several text input fields: 'Sheet number' (pre-filled with '600'), 'Title', 'Unit', 'Subunit', 'Author', 'Design date' (pre-filled with '12/17/2007'), 'Revision' (pre-filled with '0: First issue'), and 'Drawing number'. The right section, titled 'Block type', contains five radio button options: 'Comment block', 'FLD index', 'Tagnumber index', 'Program block', 'Function block', and 'Equation block' (which is selected). Below the 'Block type' section is a 'Revisions...' button. At the bottom of the dialog are five buttons: 'Import file', 'View file', 'OK', 'Cancel', and 'Help'.

| | |
|-----------------------|---|
| Sheet number | Unique number identifying the current sheet. The sheet number cannot be changed in this window. Use the FLD > Renumber FLD option to change the sheet number of the FLD. |
| Title | Name of the FLD. |
| Unit | Describes the unit the FLD is applicable to. |
| Subunit | Describes the sub unit the FLD is applicable to. |
| Author | Author of the FLD. The author name cannot be changed in this window. Use the Revisions button to change the author name for this FLD. |
| Design date | Date that the FLD was created. |
| Block type | Type of FLD used for the current FLD. For more information regarding FLD types, see “FLD types” on page 187. |
| Revisions | <p>An overview is given of the revisions of the current FLD.</p> <p>New revisions can be added with the Add button.</p> <p>Revisions can be deleted with the Delete button.</p> <p>For each revision, the revision number, date, author and description can be edited.</p> <p>For more information, see “Creating Revisions” on page 219.</p> |
| Drawing number | Identifies the drawing number as shown on the printout. Up to 25 characters are allowed for drawing number. |

Import file

Opens a dialog to import an equation table that has been created before. Note that this button is only visible when you have selected an equation block.

For information on creating equation tables see “Creating equation blocks” on page 210.

View file

Displays the content of an equation table selected for import. Note that this button is only visible when you have selected an equation block.

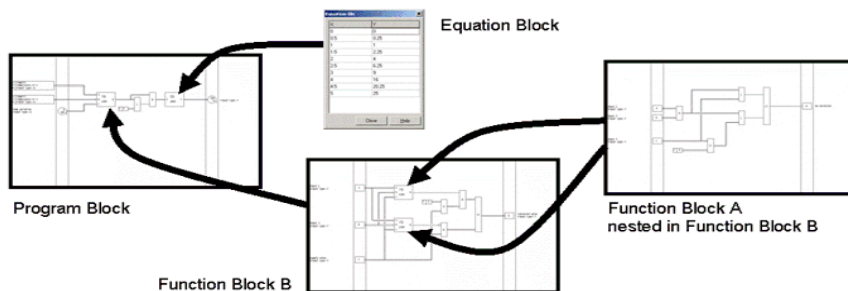
Nesting FLDs

Function blocks and Equation blocks can be nested in other FLDs. Nesting means that the FLD can be embedded as part of another FLD.

You can nest Function blocks and Equation blocks in other Functions blocks which, on term, can be nested in other Function blocks or Program blocks.

When nesting Function blocks or Equation blocks, note that the FLD number of the nested FLD must be *higher* than the FLD you are going to nest into.

Figure 26 Nesting FLDs



Importing FLDs

**Attention:**

When you change, redraw, disconnect, relocate existing logic on FLDs or import entire FLDs, the embedded compiler markers and registers may be removed or regenerated, thus affecting the actual field states during an OLM.

Note that renumbering FLDs does not affect the field states during an OLM.

During an OLM the following should be considered:

- **All new or regenerated points on a modified FLD start with their power-up value.** This includes all regenerated compiler markers and registers and all imported and copied logic.

With the **Import FLDs** wizard you can:

- import multiple FLDs from another SM Controller.
- copy multiple FLDs within the same SM Controller.



Notes:

1. When you choose to also import the IO points of the imported FLDs, you might create duplicate points. To prevent this all duplicate points get the prefix `COPY_OF_`.
 2. When you import an FLD the wizard also selects the corresponding function and equation blocks for import.
*If **Import FLD** needs to import a function or equation block to an already occupied destination, the wizard will assume that this function or equation block has already been imported in an earlier stage.*
 3. Function and equation blocks can be renamed but not renumbered during import.
 4. A *completed* import action cannot be rolled-back or undone.
-

To start the **Import FLDs** wizard, choose **FLD > Import FLDs** from the menu bar.

The wizard consists of 3 main steps handled by the following 3 pages:

- Page 1 - Select FLDs.
This page helps you select the FLDs you want to import.
- Page 2 - Rename & renumber selected FLDs
This page helps you to rename and renumber the FLDs you want to import.
- Page 3 - Import selected FLDs
This page imports the FLDs and checks for errors.

Page 1 - Select FLDs



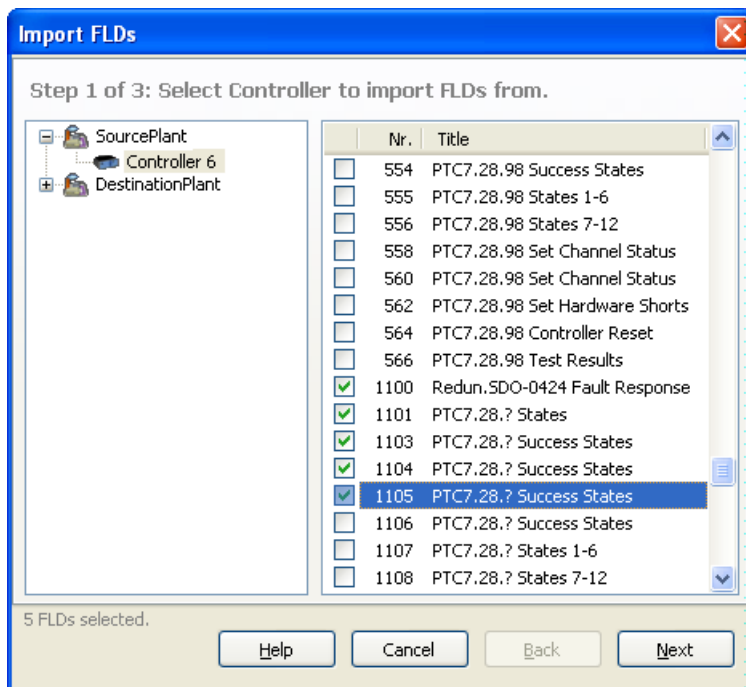
Tip:

CTRL+A selects all FLDs within the pane.

SHIFT+CTRL+A deselects all FLDs within the pane.

Figure 27 on page 197 shows that in the first page of the Import FLD wizard you select the FLDs you want to import.

Figure 27 Import FLD wizard page 1



- 1 In the left pane select the Plant and Controller you want to import from.
- 2 In the right pane select the FLDs you want to import from that Controller.
- 3 Click **Next** to process these FLDs in "Page 2 - Rename & renumber selected FLDs" on page 197.

Page 2 - Rename & renumber selected FLDs



Attention:

1. If **Import FLD** needs to import a function or equation block to an already occupied destination, the wizard will assume that this function or equation block has already been imported in an earlier stage: A message is placed in the import log and that function or equation block is *not* imported again.
It is the users responsibility to guarantee that the function and equation blocks in both source and destination application are equally numbered and contain the same version of that function or equation.
2. When you import another FLD with an existing number, the entire import will be canceled.
When renumbering selected FLDs make sure that the selected FLD locations are unused in the destination SM Controller.

Figure 28 on page 198 shows that in the second page of the Import FLD wizard you can rename and renumber the FLDs you want to import.

Figure 28 Import FLD wizard page 2

| Nr. | New Title | Original Title |
|------|-------------------------------|-------------------------------|
| 1500 | Redun.SDO-0424 Fault Response | Redun.SDO-0424 Fault Response |
| 1501 | PTC7.28.? States | PTC7.28.? States |
| 1503 | PTC7.28.? Success States | PTC7.28.? Success States |
| 1504 | PTC7.28.? Success States | PTC7.28.? Success States |
| 1505 | PTC7.28.? Success States | PTC7.28.? Success States |
| 2406 | FR:Digital Outputs | FR:Digital Outputs |
| 2499 | PST PULSE | PST PULSE |

You must step through the options in Figure 28 on page 198 from top to bottom:

- 1 In **Start FLD Number** provide the FLD number of the first FLD to be imported.
- 2 In **Step Size** select the incremental step size you want to adhere during import.
- 3 **Copy IO points from source** provides the option to import all points:
 - a. If you check this box, all IO points from the source FLD will be imported. Duplicate points will get the prefix `Copy_of_`. If prefix plus tagname exceeds the maximum tag length the prefix is shortened.
 - b. If you uncheck this box, all IO points on the imported FLDs have to be assigned manually.
- 4 Where needed, manually adjust individual FLD numbers in the *Nr.* column.
- 5 Where needed, manually adjust FLD titles in the *New Title* column.
- 6 Click **Start** to start the import on “Page 3 - Import selected FLDs” on page 199.

Page 3 - Import selected FLDs



Attention:

1. When you try to import a function block or equation block with an existing number the import of that block will be ignored and a message is stated in the log.
2. When you try to import another FLD with an existing number, an error is generated and the entire import will be canceled.

Figure 29 on page 200 shows that page 3 of the Import FLD wizard visualizes the import progress by means of a log.

The log can contain 4 types of messages:

- **Standard messages**
Standard messages contain general progress reports, they may be ignored.
- **Remarks**
Remarks are messages that do not impact the import action but may require your attention.
- **Warnings**
Warnings are messages that do not impact the import action but do require your attention.
- **Errors**
Errors are messages that indicate conflicts during import.
If an error is found the entire import action is cancelled eventually, although the wizard initially continues to see if it can collect more errors for you to resolve in one run.



Note:

When you import a large number of FLDs the wizard may take some time.

In this page of the wizard you can follow the progress of the import via the messages as shown in Figure 29 on page 200.

While the wizard is importing the **Cancel** button is changed in an **Abort** button.

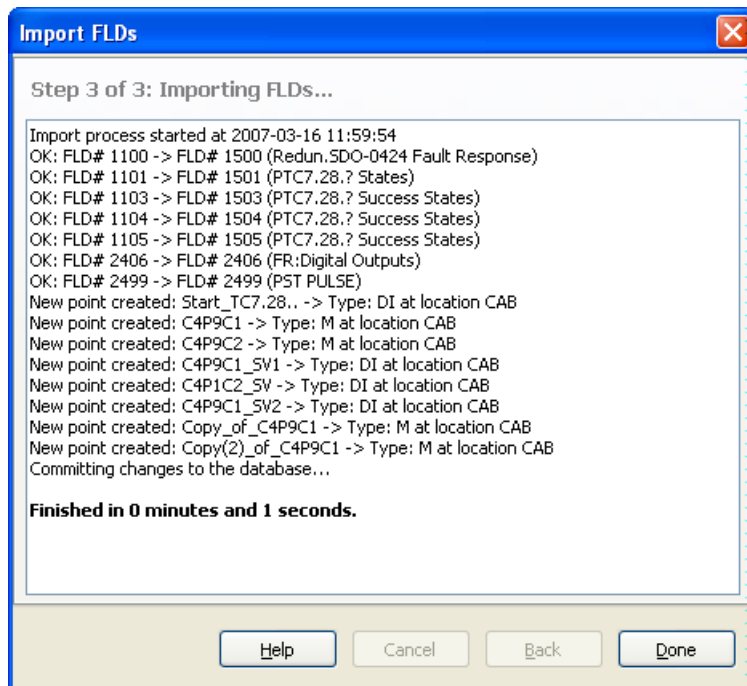
To abort during an ongoing import action:

- 1 click **Abort** to abort an ongoing import
 - a. click **Back** to correct errors and restart the import action or
 - b. click **Cancel** to undo, exit and roll-back the import action

When the wizard has finished the import was successful or errors were found:

- 1 In case of errors:
 - a. click **Back** to correct errors and restart the import action or
 - b. click **Cancel** to exit the wizard without implementing changes.
- 2 In case of successful import:
 - a. copy the log from the wizard page and save it using a word processor.
 - b. press **Done** to finish the wizard.

Figure 29 Import FLD wizard page 3



Adding logic symbols

Application Editor offers you many tabs with subsets of logical symbols you can use to add logic symbols on an FLD.

For some symbols you need to fill in a properties window before they can be added.

Connection lines



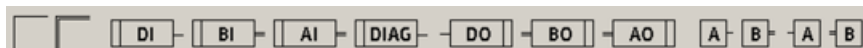
Connection lines are used to interconnect logical symbols. Connection lines are displayed on every symbol tab.

To select, click on a connection line or use a shortcut key:

- Press **S** to select a single line, used to interconnect boolean signals
- Press **D** to select a double line, used to interconnect binary signals.

For detailed information see “Connection lines” on page 346.

IO symbols



IO Symbols are used to link FLDs inputs and outputs with IO points or Function Blocks.

To select, click the **IO symbols** tab in the Application Editor and click a symbol.

Not all IO symbols are always available; Table 7 on page 201 shows the availability of IO symbols related to the type of FLD selected. For detailed information see “IO symbols” on page 347.

Table 7 Availability of IO symbols per type of FLD

| Type of IO symbol | program block | function block | comment block |
|-------------------------------|---------------|----------------|---------------|
| Digital input | available | available | available |
| Binary input | available | available | available |
| Analog input | available | available | available |
| Diagnostic input | available | available | available |
| Digital output | available | | available |
| Binary output | available | | available |
| Analog output | available | | available |
| Function block boolean input | | available | available |
| Function block binary input | | available | available |
| Function block boolean output | | available | available |

Table 7 Availability of IO symbols per type of FLD (*continued*)

| Type of IO symbol | program block | function block | comment block |
|------------------------------|---------------|----------------|---------------|
| Function block binary output | | available | available |

Assigning points

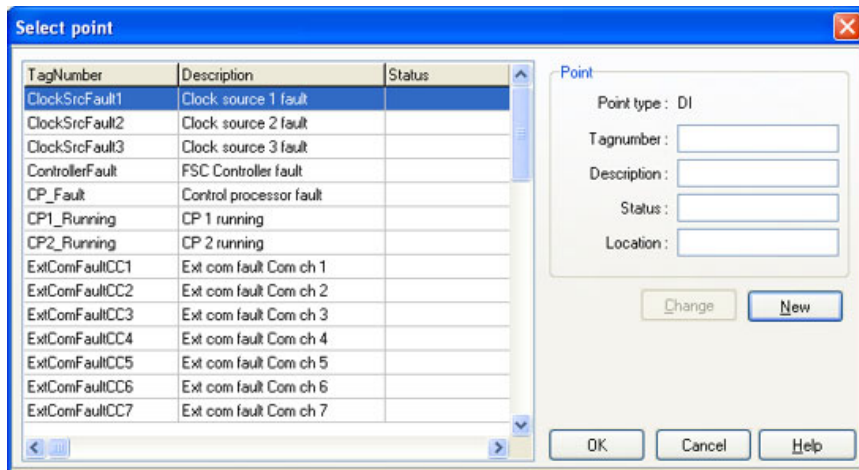
When placing an IO symbol, not being a function block IO symbol, a point has to be assigned before compiling the application. All IO points defined in the Point Configurator can be used once.

Depending on the state of a point assigned, the color of the symbol changes:

- Non-safety related points are displayed in blue,
- safety related points are displayed in red.

When you place an IO symbol on the FLD, a window might pop up in which you must:

- select the point the IO symbol refers to or,
- create a new point (click the **New** button). If you create a new point it will be added to the point database.



The left side of the window lists all available points.

Point type

Displays the type of the selected point.
For more information see “Point Type” on page 393.

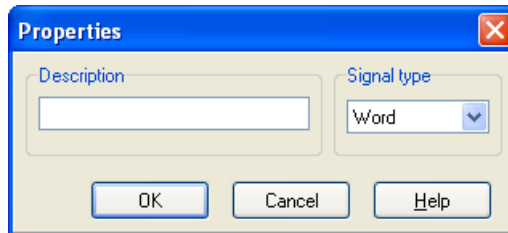
Tagnumber

Displays the Tag number of the selected point.
For more information see “Tag number” on page 394.

Description

Displays the Description of the selected point.
For more information see “Description” on page 394.

| | |
|----------------------|--|
| Status | Displays the Status of the selected point. For more information see “Status” on page 394. |
| Location | Displays the Location of the selected point. For more information see “Location” on page 394. |
| Register type | Displays the Register type of the selected point. For more information see “Register type” on page 400. |
| Change | Use this button to change some properties (Tag number, Description, Status, Location, Register type) of the selected point. After changing the properties, accept the changes with the OK button. |
| New | Use this button to create a new point, instead of choosing one from the list. You can define some properties of the point (Tag number, Description, Status, Location, Register type) and configure the other properties later in the Point Configurator. |
| OK | Links the selected point to the IO symbol. |
| Cancel | Closes the current window. |



For Function block inputs and outputs, the following properties can be defined:

| | |
|--------------------|---|
| Description | Available for all Function block inputs and outputs. Displays the Description of the selected point. For more information see “Description” on page 394. |
| Signal Type | Available for Function block binary inputs and outputs. For more information see “Register type” on page 400. |

Sheet transfers



Sheet transfers are used to connect the output of one sheet with an input of another.

Sheet transfers are available on Program Blocks and Comment Blocks. For detailed information see “Sheet transfers” on page 351.

To select, click the **Sheet Transfers** tab in the Application Editor and click a symbol.

The following sheet transfers can be used:

- Boolean on-sheet transfer
- Binary on-sheet transfer
- Boolean off-sheet transfer
- Binary off-sheet transfer
- Multiple boolean off-sheet transfer
- Multiple binary off-sheet transfer

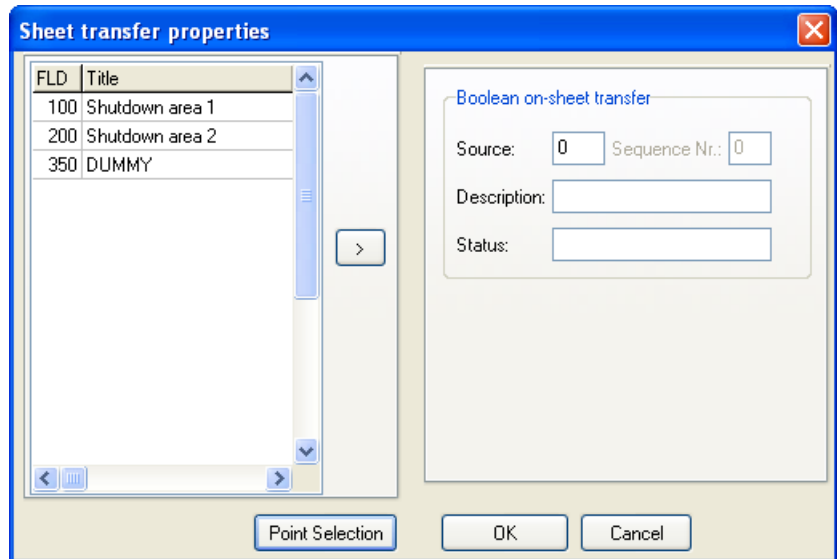
An on-sheet transfer on one FLD is linked to an off-sheet transfer on another FLD. Each sheet transfer shows the following parameters in its symbol on screen:

| | |
|------------------------|--|
| source | The sheet number from which the signal leaves the FLD. |
| destination | The sheet number in which the signal enters the FLD. |
| sequence number | In case of multiple sheet transfers between two FLDs, the sequence number distinguishes these sheet transfers. |

Sheet transfers operate in pairs: an off-sheet transfer on one FLD needs an on-sheet transfer on another FLD in order to work properly.

If, for example, on the FLD with sheet number = 2 an off-sheet transfer is placed to the FLD with sheet number = 3, an on-sheet transfer is automatically added to the FLD with sheet number = 3. Both of these transfers will have Source = 2 and Destination = 3.

When a sheet transfer is chosen, a window similar to the one displayed below appears.



The left window lists all possible sheets that act as destination or source sheet, depending on the type of transfer that is added. You can select the desired destination/source sheet and click “>”. Then you can add some details like Description and Status as a reference.

Point Selection/ FLD Selection

Toggles between **Point Selection** and **FLD Selection**.

FLD Selection is used to choose a specific source/destination FLD.

A transfer is placed on the current FLD as well as on the source/destination FLD to form a working pair.

Point Selection is used to choose an existing source/destination point. In that case, a transfer is placed to the chosen transfer point to form a working pair.

Source / Destination

The FLD sheet number the transfer refers to/from.

Sequence Nr.

If more transfers occur between two specific FLDs, they are distinguished by a sequence number.

Description

A description of the transfer, to be entered by the user.

Status

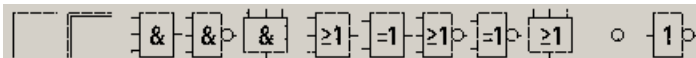
A status description of the transfer, to be entered by the user.

Signal type

Only available in case of Binary transfers, this contains the signal type: Word, Byte, Long or Float.

Sheet x:, Sequence Nr x: Only available in case of multiple sheet transfers, this enables the user to make an off-sheet transfer to up to five on-sheet transfers. If, for example, transfers are made to sheets 15 and 20, this will be notated alongside the transfer symbol as “To 20,30”.

Logical functions



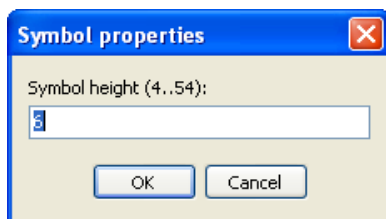
This tab contains all the “basic” logical functions for comparing boolean signals.

The following logical functions can be used:

- AND gate
- NAND gate
- Rotated AND gate
- OR gate
- XOR gate
- NOR gate
- XNOR gate
- Rotated OR gate
- Inverter
- Buffer inverter

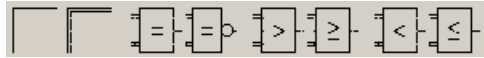
For detailed information see “Logical functions” on page 353.

When you add an AND gate, NAND gate, OR gate or NOR gate, you will be asked for the symbol height or symbol width (when adding a rotated symbol).



This value represents the number of connection lines (both inputs and output) that can be connected to the symbol.

Compare functions



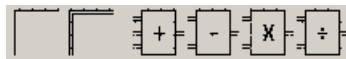
This tab contains the logical functions for comparing binary signals.

The following compare functions can be used:

- EQUAL gate
- NOT EQUAL gate
- GREATER THAN gate
- GREATER THAN OR EQUAL gate
- LESS THAN gate
- LESS THAN OR EQUAL gate

For detailed information see “Compare functions” on page 356.

Calculation functions



This tab contains operators that you can use to perform basic mathematical operations.

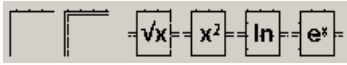
The following calculation functions can be used:

- ADDITION gate
- SUBSTRACT gate
- MULTIPLY gate
- DIVIDE gate

For detailed information see “Calculation functions” on page 358.

When you add an ADDITION gate, you will be asked for the symbol height. This value represents the vertical size of the symbol.

Mathematical functions



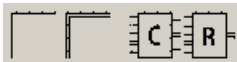
This tab contains operators that you can use to perform advanced mathematical operations.

The following mathematical functions can be used:

- SQUARE ROOT gate
- SQUARE gate
- NATURAL LOGARITHM gate
- EXPONENT gate

For detailed information see “Mathematical functions” on page 360.

Counters and registers



This tab contains operators that you can use for counting functions (counters) and for storing values (registers).

The following counters and registers can be used:

- COUNTER
- REGISTER

For detailed information see “Counters and registers” on page 362.

- When you add a COUNTER you will be asked to enter the maximum value of the counter.
- When you add a REGISTER you will be asked to choose a register type (Byte, Word, Long or Float).

Constants and Signal converters



This tab contains operators that output a constant value to the logic (constants) or convert the value of the input to a desired output type (converters).

The following constants and signal converters can be used:

- CONSTANT VALUE
- CONSTANT BOOLEAN
- SIGNAL CONVERSION

For detailed information see “Constants and signal conversions” on page 365.

When you add a CONSTANT VALUE you have to enter the constant type (Byte, Word, Long or Float) and the value of the constant.

When you add a SIGNAL CONVERSION you have to enter the desired Source (Word, Long or Float) and Destination (Byte, Word or Long). The following table displays the possible conversions:

Table 8 Signal conversion

| | | Destination | | |
|--------|-------|-------------|------|------|
| | | Byte | Word | Long |
| Source | Word | Yes | No | No |
| | Long | Yes | Yes | No |
| | Float | Yes | Yes | Yes |

Function and equation blocks



This tab contains Function blocks and Equation blocks.

For more information see “Function and equation blocks” on page 367.

Function blocks

Function blocks can only be used in a certain FLD after one or more other FLDs of the type Function Block have been created.

When you add a Function block, a window will appear listing all available Function blocks, so you can choose which Function block to use.

If only one Function block is defined, that Function block is used automatically when adding a Function Block.

To create function blocks see “Creating function blocks” on page 210.

To nest Function blocks see “Nesting FLDs” on page 195.

Equation blocks

Equation blocks can only be used in a certain FLD after one or more other FLDs of the type Equation Block have been created.

When you add an Equation block, a window will appear listing all available Equation blocks, so you can choose which Equation block to use.

If only one Equation block is defined, that Equation block is used automatically when adding an Equation Block.

To create equation blocks see “Creating equation blocks” on page 210.

To nest Equation blocks and Function blocks see “Nesting FLDs” on page 195.

Creating function blocks



Attention:

All FLDs with an FLD number, higher than the one you create for this function block *must* also be used for equation or function blocks.

You can only create function blocks on FLDs numbered 500 or higher.

- 1 Create a new FLD with FLD number 500 or higher as described in “Creating a new FLD” on page 190.
- 2 Select **Equation block** as block type in **FLD Properties**, as described in “FLD properties” on page 193.
- 3 Create the logic function of the function block as described in “Drawing logic” on page 216.

Creating equation blocks



Note:

After the values are imported the original table is no longer required. It is advised however to keep the equation table available for future modifications.

To create or modify an equation block you must first create an equation table which can be imported in the equation block.

The equation table is an externally created file with a certain format, used to import the **x** and **y** values into the equation block.

Once an equation table has been created, you can import the equation table as described in “Importing equation tables” on page 214.

Equation table format

The equation table consists of two columns. The first column contains the input (**x**) values, and the second column the output (**y**) values. A row with an **x** and **y** value forms a point pair (**x**, **y**).

The following syntax rules apply when creating an equation table:

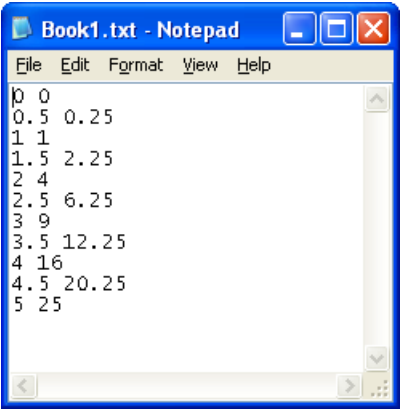
1. The equation table is of type *.txt, ANSI encoded (text document), or *.prn (formatted text, space delimited).
2. Each line in the equation table must contain an input and an output value with at least one space between them.
3. Empty lines and tabs are not allowed in an equation table.
4. The equation table shall have at least 3 rows, the maximum number is 200.
5. The input values must be in a low to high numerical order.
6. Normal and exponential notations may be used. For example, 0.05 is the same as 5.0E-2.¹
7. The input values (**x**) and output values (**y**) must be between -10^{38} and $+10^{38}$.

1. When using European notation, the dot separation symbol is to be replaced by a comma.

Creating an equation table using Notepad

Figure 30 on page 212 shows an example of a correct equation table designed with Notepad.

Figure 30 Example of an equation table designed with Notepad



- 1 Open Notepad with an empty sheet.
- 2 Type the input value (**x**), followed by a space to separate the input value (**x**) from the output value (**y**).
- 3 Type the output value (**y**) on the same line.
- 4 Press **Enter** to go to the next line.
- 5 Go back to step 2 on page 212, until all values are entered. Do not add empty lines or comments.
- 6 Save as *.txt file using ANSI encoding (default).
- 7 Import the equation table in an equation block as described in “Importing equation tables” on page 214.

Creating an equation table using Excel

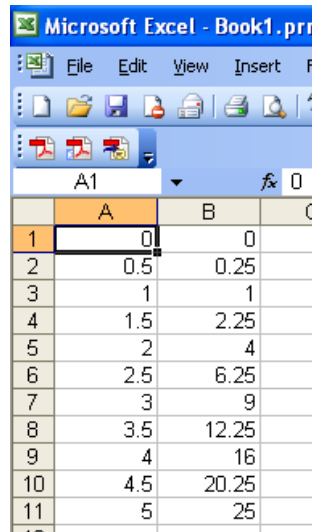


Tip:

Excel gives you the benefit of using formulas and copy functions to set the input and output values.

Figure 31 on page 213 shows an example of a correct equation table designed with Excel.

Figure 31 Example of an equation table designed with Excel.



| | A | B | C |
|----|-----|-------|---|
| 1 | 0 | 0 | |
| 2 | 0.5 | 0.25 | |
| 3 | 1 | 1 | |
| 4 | 1.5 | 2.25 | |
| 5 | 2 | 4 | |
| 6 | 2.5 | 6.25 | |
| 7 | 3 | 9 | |
| 8 | 3.5 | 12.25 | |
| 9 | 4 | 16 | |
| 10 | 4.5 | 20.25 | |
| 11 | 5 | 25 | |

Below steps indicate how to create an equation table using Excel:

- 1 Open a blank sheet in Excel.
- 2 Place the first input value (**x**) in cell A1.
- 3 Place at least 2 more input values in the underlying rows (A2, A3, etc.), but do not continue beyond cell A200. Do not skip any rows. Use a formula as desired.
- 4 Place a formula in cell B1 that calculates the output value (**y**) from the input value (**x**) in cell A1.
- 5 Copy the formula to all underlying rows containing an input value (**x**).
- 6 Save the Excel sheet for later reference.
- 7 Save the Excel sheet with extension `*.prn`; this format can be imported as an equation table.
- 8 Import the equation table in an equation block as described in “Importing equation tables” on page 214.

Importing equation tables



Attention:

All FLDs with an FLD number, higher than the one you create for this equation block *must* also be used for equation or function blocks.

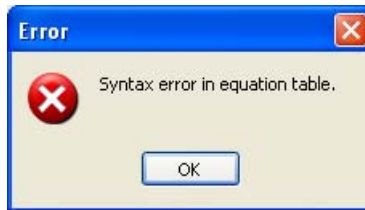
You can only import an equation table on FLDs numbered 500 or higher.

- 1 Create a new FLD with FLD number 500 or higher as described in “Creating a new FLD” on page 190.
- 2 Select **Equation block** as block type in **FLD Properties**, as described in “FLD properties” on page 193.
- 3 Click the **Import file** button and open the equation table. To create an equation table see “Creating equation blocks” on page 210.

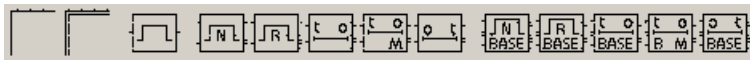
If the format of the equation table is not correct while attempting to import the table, a message as shown in Figure 32 on page 214 is displayed.

- 4 Fill the sheet details such as *Title*, *Unit* and *Subunit* and click **OK**.

Figure 32 Message displayed when importing a faulty designed equation table



Timers



This tab contains various types of timers.

The following timers can be used:

- Pulse
- Timers with constant timer value: pulse
- Timers with constant timer value: pulse retriggerable
- Timers with constant timer value: delayed ON
- Timers with constant timer value: delayed ON memorize

- Timers with constant timer value: delayed OFF
- Timers with variable timer value: pulse
- Timers with variable timer value: pulse retriggerable
- Timers with variable timer value: delayed ON
- Timers with variable timer value: delayed ON memorize
- Timers with variable timer value: delayed OFF

For detailed information see “Timers” on page 371.

When you add a timer with a constant timer value, you will have to specify the **Timer Base** (10 ms, 100 ms, s, min) and **Timer Value**.

When you add a timer with a variable timer value, you will have to specify the **Timer Base** (10 ms, 100 ms, s, min).

Flip-flops



This tab contains various types of flip-flops.

The following flip-flops can be used:

- S-R flip-flop
- R-S flip-flop

For detailed information see “Flip-flops” on page 378.

Non-functional symbols



This tab contains various types of non-functional symbols. These symbols have no impact on the functioning of the FLD.

The following non-functional symbols can be used:

- Revision cloud
- Texts

For detailed information see “Non-functional symbols” on page 380.

Drawing logic

Warning

When creating logic, make sure that calculation limits and value ranges are adhered to *at all times* during execution of the logic.

Adding a symbol

To add a symbol to an FLD, click the relevant symbol in the symbol library. The symbol is immediately added. Use the mouse to move the symbol to the correct location and click it to fix it there.

To add a symbol to an FLD, identical to the last selected symbol, choose **FLD > Last Symbol** or type the shortcut key **L** on your keyboard. (For more shortcut keys see “Application Editor shortcut keys” on page 186). The symbol is immediately added.

Use the mouse to move the symbol to the correct location and click it to fix it there.

Drawing connection lines



Tip:

You can draw lines faster by using the shortcut keys **S**, **D** and **L** on your keyboard. For details see “Application Editor shortcut keys” on page 186.

To draw connection lines between symbols:

- 1 Select the relevant connection line from the symbol library (available in any tab of the symbol library). Use a single line for boolean data or use a double line for analogue data.
- 2 Click the starting point of the connection line.
- 3 Route the connection line to the end point. You can use the left mouse button to make corners or connect the line to a symbol. You can use the right mouse button to end the line.

Moving symbols



Tip:

The easiest way to move a symbol is to right-click the symbol and move the mouse with the right mouse button held down.

When you move a symbol, you change its location but leave the connection lines in place.

To do so, right-click the symbol and select **Move** or type the shortcut key **M** on your keyboard. Move it to the correct location and left-click it to fix its location.

Because connection lines are disconnected, moving allows you to move a symbol to any location within the drawing area of the FLD.

Dragging symbols



Tip:

The easiest way to drag a symbol is to left-click the symbol and move the mouse with the left mouse button held down.

When you drag a symbol, you change its location but leave the connection lines intact (attached to the symbol).

To do so, right-click the symbol and select **Drag** or type the shortcut key **R** on your keyboard. Drag it to the correct location and left-click it to fix its location.

Because connection lines are kept attached, movement by dragging is restricted.

Copying symbols

To copy a symbol, right-click it and select **Copy** or type the shortcut key **C** on your keyboard. A copy of the symbol will then appear, which you can place at the desired location with a left-click.

Working with blocks

A block is an area on an FLD containing (part of) a logic function.

Blocks are useful to copy, delete, save or move entire pieces of logic.

Selecting blocks

To select a block drag the mouse from one corner of the block to the opposite corner while holding down the left mouse button.

- Releasing the mouse button will end the selection process.
- A dotted rectangle indicates the size and location of the selection.



Warning:

Components must be *completely* embraced by the selection to be part of a block.

Processing blocks

You can copy delete or move a block by right clicking inside a selected block.

Saving and loading blocks

To save part of an FLD as a block, select it by dragging over it with the mouse. Then, right-click and choose **Save**. The selection is saved as an .BLK file.

To load a previously saved block in an FLD, choose **FLD > Load block** (or click the **Load block** button or press **CTRL+B**), and choose the saved BLK to place it in the selected FLD. The block is immediately added. Use the mouse to move the block to the correct location and click it to fix it there.

Deleting symbols



Attention:

When you delete a point of type DI, BI, AI, DO, BO or AO from an FLD, the point is *not* deleted from the point database.

On the other hand: logic symbols containing points, such as timers (T) and registers (R) *are* removed from the point database when deleted from an FLD.

To delete a symbol from the FLD, right-click the symbol and select the **Delete option** or type the shortcut key **D** on your keyboard. After confirmation, the selected symbol is deleted from the current FLD.

Changing symbols

Some symbols (for example timers or registers) have parameters that can be changed. To do so right-click the symbol and select **change** or type the shortcut key **H** on your keyboard. Then a window will appear in which you can select a new symbol. For some symbols, like inputs or outputs, it is also possible to select a new point by clicking **change**.

Properties of symbols

From some symbols (for example input and output) you can change the properties. To do so right-click a symbol and select **properties** or type the shortcut key **P** on your keyboard. This will open the **Configure Point** window. Here, you can change the attributes of the point this input or output refers to. For more information see “Allocating points” on page 160.

Creating Revisions



Attention:

The revisions as described here are *not* part of, or automatically updated by Audit Trail.

Application Editor automatically assigns a revision ID to each created FLD.

A revision ID consists of an ID number, an author and a description and is used to identify changes made to the application.

- The revision ID number of an FLD is included in the FLD index.
- The revision history of an FLD is shown on printouts of an FLD.

When creating, updating or revising an application you should also update the revision ID.

There are two ways to update an revision ID:

1. Update the revision ID spanning all FLDs, see page 219.
2. Update the revision ID of a single FLD, see page 220.

Update the revision ID spanning all FLDs

When you update the revision ID of all FLDs, you set the revision ID of all FLDs to the value of the FLD with the highest revision number.

To do so, click **FLD>Application revision** from the menu.

This will open a window **Latest revision on FLD: x** where **x** is the FLD with the highest revision number:

| No. | Date | Author : | Description |
|-----|-----------|----------|-------------|
| 0 | 4/28/2006 | | First issue |
| 1 | 5/8/2006 | | |

OK Cancel Help

In this window, the first line shows the fields of the highest revision ID.

The second line can be used to set *all FLDs* to a new, higher revision. In this second line the revision number, date, author and description can be edited.

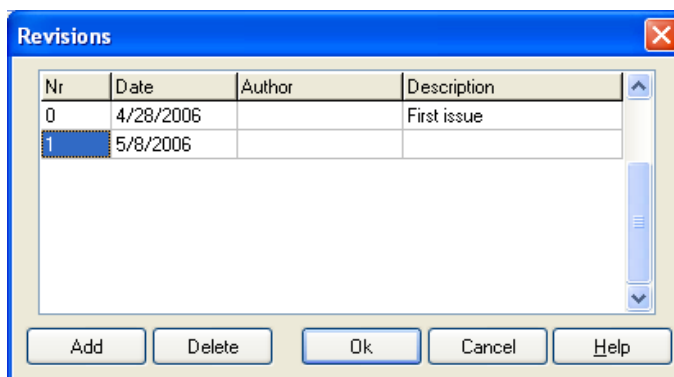
Clicking **OK** will set all FLDs to this new revision.

Update the revision ID of a single FLD

To set the revision ID of a single FLD, act as follows:

- 1 Select the FLD concerned
- 2 Open the **FLD properties** (see “FLD properties” on page 193)
- 3 Click the **Revisions** button to open a second window as shown in Figure 33 on page 220.
- 4 You now have the following options:
 - a. Click **Add** to create a new Revision ID.
 - b. Fill/modify the **Date**, **Author** and the **Description** field.
 - c. Click **Delete** to delete a Revision ID (You cannot delete revision 0!).
- 5 Click **OK** when done, or **Cancel** to abort.

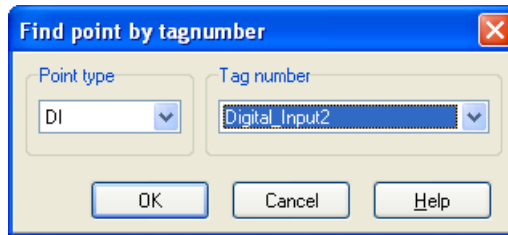
Figure 33 Update the revision ID of a single FLD



Finding points

To discover on which FLD a specific point is used, you can use the option Configure point in the Point Configurator (see “Configuring a point” on page 158).

You can also use the **Find Point** function of the Application Editor. To access this function choose **FLD > Find Point** from the menu. The following window will then appear:



Since any point can be identified by the unique combination of point type and Tag number, these two parameters can be chosen in the Find point window:

| | |
|-------------------|---|
| Point type | Here you select the type of the point you want to find. |
| Tag number | Select the tag number of the point you are looking for. |
| Cancel | Cancels the find action and closes the Find point window. |
| OK | Opens the FLD where the point was found (and closes the Find point window). |

Printing

You can print one or more FLDs.

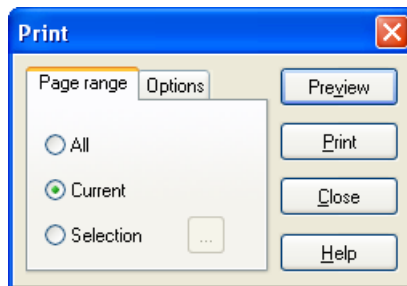
To access this function you can either:

- Click the **Print** button in the toolbar
- In the menu select **File > Print**

Print - Pages

This dialog lets you select the pages you want to print.

You can access this window by selecting **File > Print** in the menu and then selecting the **Pages** tab.

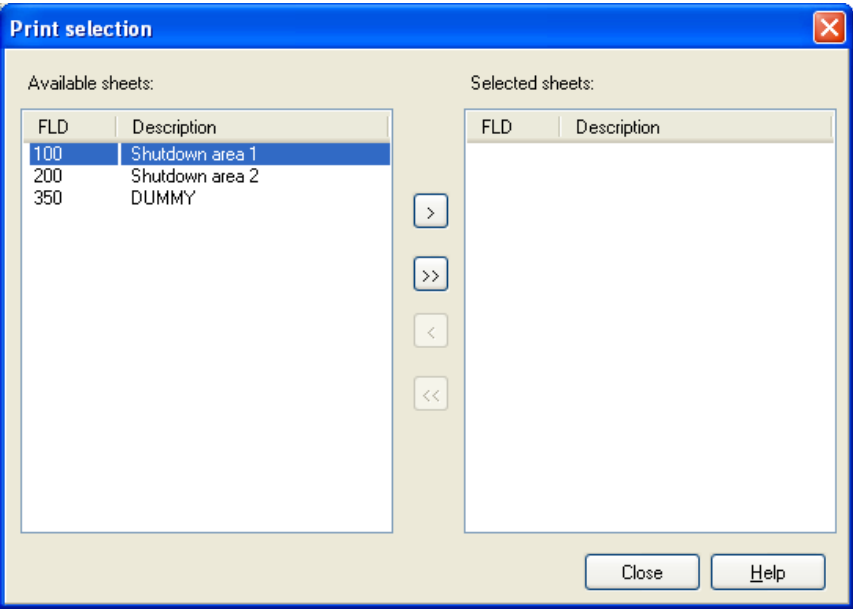


All

Prints all FLDs.

| | |
|------------------|----------------------------------|
| Current | Prints only the current FLD. |
| Selection | Selects which FLDs to print. |
| Preview | Displays a preview of the print. |
| Print | Starts printing. |

If you choose the **Selection** option and click the “...”-button the following window will appear:

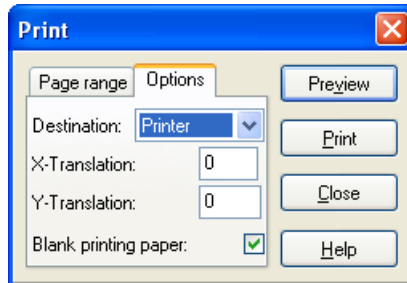


| | |
|-------------------------|--|
| Available sheets | A list of all sheets available for printing. |
| Selected sheets | A list of all sheets that will be printed, which is a selection of all available sheets. |
| > | Move the selected sheet from available sheets to selected sheets . |
| >> | Move all sheets from available sheets to selected sheets . |
| < | Move the selected sheet from selected sheets to available sheets . |
| << | Move all sheets from selected sheets to available sheets . |

Print - Options

This dialog lets you modify the options of the print job.

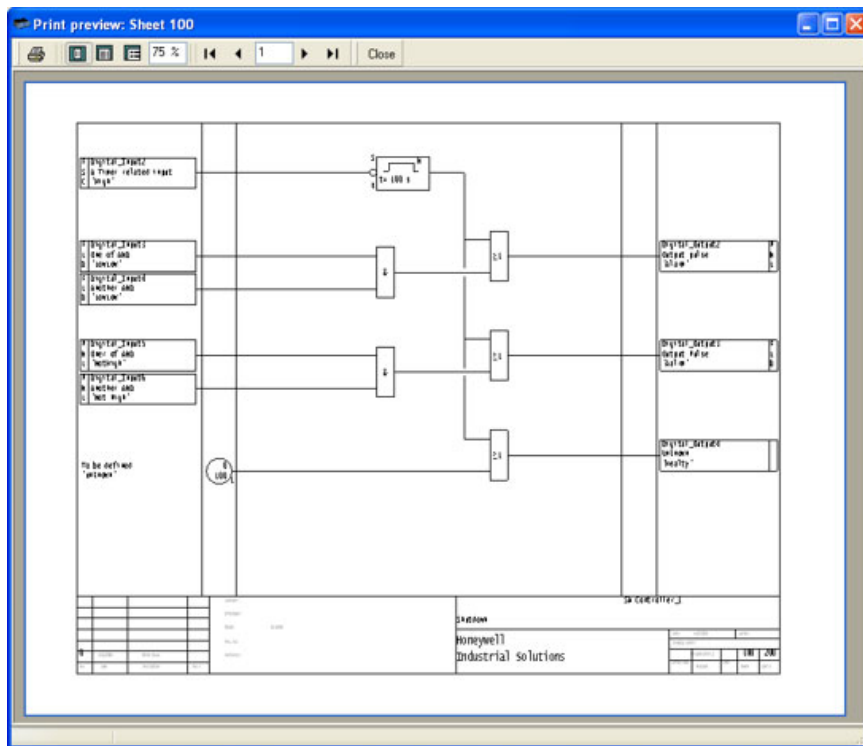
You can access this window by selecting **File > Print** in the menu and then selecting the **Options** tab.



| | |
|-----------------------------|---|
| Destination | You can choose to send the print job to either a printer or a file (HPGL format). |
| X-Translation | Allows you to horizontally position the FLD on the paper. The value must be entered as points (28 pts = approx. 1 cm; 72 pts = approx. 1 inch) and may be positive or negative. A value of 0 means the FLD is aligned to the left side of the paper. Positive values move the FLD to the right, negative values move the FLD to the left. |
| Y-Translation | Allows you to vertically position the FLD on the paper. The value must be entered as points (28 pts = approx. 1 cm; 72 pts = approx. 1 inch) and may be positive or negative. A value of 0 means the FLD is aligned to the top side of the paper. Positive values move the FLD downwards, negative values move the FLD upwards. |
| Blank printing paper | Here you specify whether you use blank paper or preprinted paper. If you use preprinted paper, no title block and sheet borders will be drawn. |
| Preview | Displays a preview of the print |
| Print | Starts printing. |

Print preview

Before printing to paper you can preview the output on screen. To do so select **File > Print** in the menu and press the **preview** button. The following window will then appear:



Place the mouse cursor above the buttons to see the texts mentioned below.

| | |
|----------------------|---|
| Print Report | Prints the report to paper with current settings. |
| Whole page | Adjusts zoom to view entire page. |
| Page width | Adjusts zoom to page width. |
| 100% | Adjusts zoom to 100%. |
| Zoom | Here you can adjust the zoom level to a custom value. Values can range from 15 to 250%. |
| First page | Browses to the first page of the report. |
| Previous page | Browses to the previous page of the report. |
| Page number | Displays current page number. Enter a page number and press Enter to go directly to that page. |
| Next page | Browses to the next page of the report. |
| Last page | Browses to the last page of the report. |
| Close | Closes the preview window. |

Using the right mouse button (right-click) on the previewed FLD gives the following options:

Copy to Clipboard

Copies the current preview of the FLD to the clipboard.

Save to File

Saves the current preview of the FLD to a file. The preview can be saved as vector graphic (*.emf) or as bitmap (*.bmp, *.jpg).

Application Compiler

An application has to be compiled first before it can be downloaded in Safety Manager.

During compilation the application is checked, which may result in error and warning messages. If no errors are found, a Controller File is created which can be downloaded in Safety Manager.

The Application Compiler uses the following information during compilation:

- Safety instrumented functions in the FLDs in combination with the symbol and function block library information.
- Hardware configuration information and points allocated to hardware.
- Communication points for exchanging data with for example other systems.
- Points not allocated to hardware or communication.
- Timing and scheduling information so Safety Manager can execute tasks in the correct sequence and within the timing constraints.

This section covers the following topics:

| Section | See |
|-----------------------------------|----------|
| Starting the Application Compiler | page 226 |
| Application Compiler menu | page 229 |
| Using the Application Compiler | page 229 |
| Creating a Controller file | page 230 |

Starting the Application Compiler

The Application Compiler can be started by:

- Selecting **Tools > Configuration > Application Compiler** in the **Menu bar**,
- Clicking the **Application Compiler** icon in the **Outlook bar**
- Pressing the shortcut keys **Alt, T, C, L**

When you start the Application Compiler, a warning as in Figure 34 on page 227 appears.



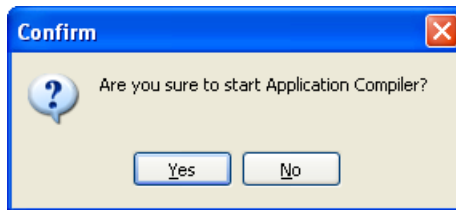
Stop

To view live data in an online Safety Manager the application version loaded in the system and in Safety Builder must be identical.

If you compile you upgrade the application version in Safety Builder. *To view live data again you must first load the upgraded Controller Files in Safety Manager.*

Alternatively you can discard this version and restore a backup (see “Backup & restore” on page 64).

Figure 34 A warning displayed when entering the Application Compiler



If you click **Yes** the Application Compiler starts compiling as shown in Figure 35 on page 228.

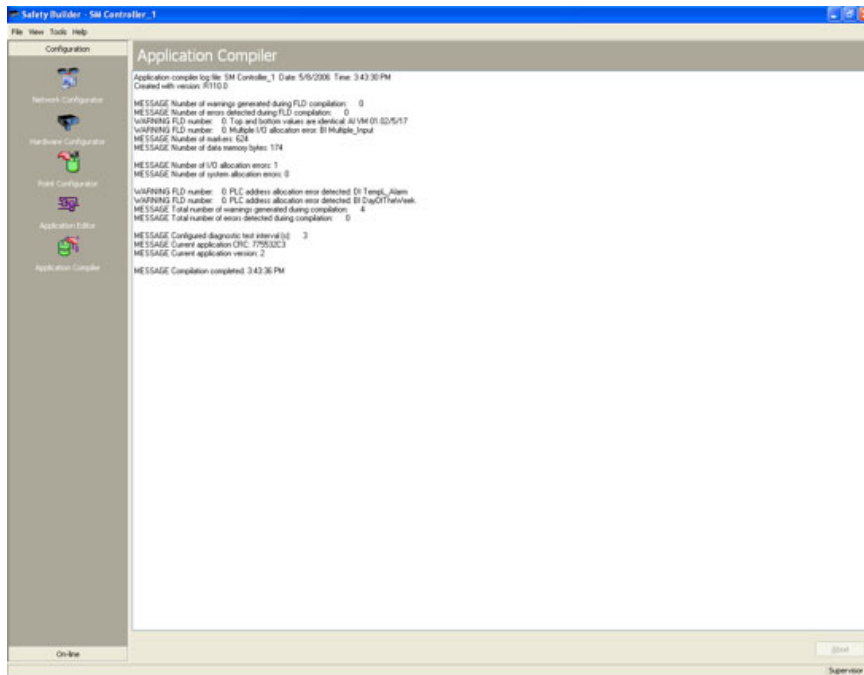


Note:

If you get a popup stating exclusive access is denied see “Working in a multi user environment” on page 228.

- Once the compilation is completed you must load the Controller File in the Safety Manager (see “Load Controller” on page 251).
- During compilation a log file is created, see “Compilation log file” on page 230 for details.
- To abort the compilation process press the **Abort** button at the bottom right corner of the screen. (See also “Stop compiling” on page 232.)

Figure 35 Application Compiler screen



Working in a multi user environment



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
 2. To give up exclusive access to an SM Controller access the **Network Configurator**.
 3. To give up shared access exit the tool or function that demands shared access.
- To give up all access you can close the file (click **File>Close** from the menu bar).

When you try to access the SM Controller with multiple users simultaneously, access via this tool may be denied and you get a popup stating either:

Access is denied, please try again later.

Exclusive access is denied, please try again later.

- If the Plant database is opened for exclusive use by someone using Network Configurator, your access to this tool is denied.
- If the SM Controller database is opened by someone, using this or a similar tool, your access to this tool is denied.

In above cases, you cannot continue until the “denied access” lock is relieved by the other user(s).

For more information see also “Multi user environment” on page 36.

Application Compiler menu

Below list shows the Safety Builder Application Compiler menu structure.

The shortcut access key combinations, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also “Keyboard shortcut and access keys” on page 32.

| Menu item | Description |
|-------------------------------|---|
| <i>File</i> | |
| > C lose | Closes the Compiler. |
| > E xit | Exits Safety Builder. |
| <i>View</i> | |
| > T oolbars | Toggles display of the toolbars. |
| > O utlook Bar | Contains short cuts to the program functions. |
| > A udit Trail Viewer | Launches the Audit Trail Viewer. |
| <i>Tools</i> | |
| > C onfiguration | Displays a sub menu with available configuration tools. For an overview see “Safety Builder configuration tools” on page 41. |
| > O n-line | Displays a sub menu with available on-line tools. |
| > P assword | Launches the Security tool. |
| > O ptions | Enables you to set general program options. |
| <i>Help</i> | |
| > S afety Builder Help | Launches the Safety Builder Help function. |
| > A bout | Shows current version and license of the program. |

Using the Application Compiler

When you open the Application Compiler it automatically starts compiling the selected Controller application.

For more information see:

- “Starting the Application Compiler” on page 226 about how to start the Application Compiler.
- “Creating a Controller file” on page 230 for more information regarding the creation details.

Application Compiler shortcut keys

Besides the shortcut keys listed in “Keyboard shortcut and access keys” on page 32 there are no shortcut keys active in Application Compiler.

Creating a Controller file

Prerequisites

Before you start compiling the configuration of the application must be free of configuration errors.

Compilation log file

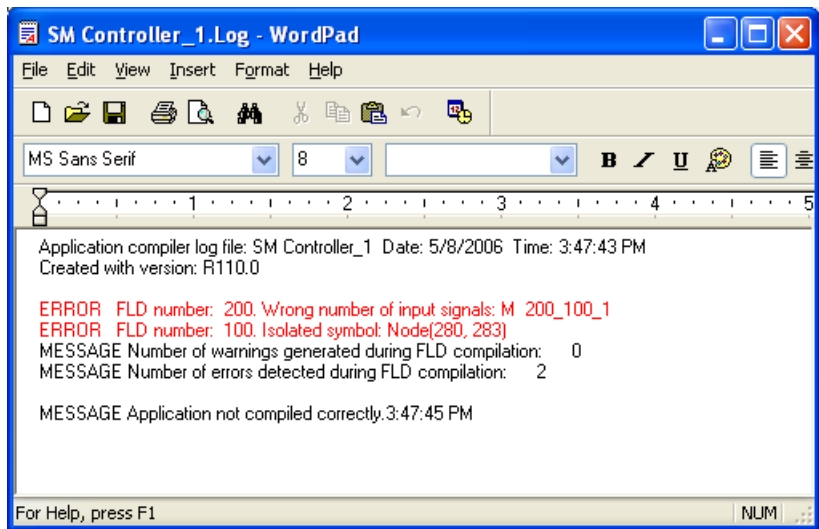
During the compilation process, a log file is made. You can use the log file to find & correct errors and, if necessary, deal with the warnings.

The log file is stored in the same directory as the controller data, and is called “<controllername>.LOG”, where <controllername> is the name of the controller whose FLDs are compiled.

To open the log file, click **View>Compilation Log File** from the **Menu bar**.

The log file is in RTF format and is accessed via WordPad.

Figure 36 Example of a log file



Compilation process

The Application Compiler of the Safety Builder translates the application for Safety Manager.



Note

The version number of an application is automatically increased during compilation. Please note that the version number of an application is also increased during a Safety Builder upgrade.

Before the application can be compiled successfully, it has to be syntactically correct.

Progress messages

The compiler checks if the application can be executed and generates & stores messages in a log file while progressing. It also generates messages if errors or warnings are detected.

Detailed information concerning message content can be found in “Application Compiler messages” on page 493.

Warning messages

Like normal progress messages, warnings are indicated as black text in the compiler progress window and log file.

The compiler generates warnings if a syntax or configuration is allowed but unexpected (for example an unconnected input of a function block). All messages are reported and logged in the log file.

Error messages

Errors are, unlike normal progress messages, indicated as red text in the compiler progress window and log file.

The compiler generates an error if a syntax or configuration cannot be executed. If an error is detected during compiling, the compiler normally continues the compilation process, meaning that some errors are reported more than once (for example if more than one signal connects to the same node).

If compile errors are found, you should solve them by making appropriate changes in the Network Configurator, Hardware Configurator, Point Configurator or Application Editor, and compile the application again, until no more errors are found. Only then a controller file is created.

Status information during compilation

During compilation, the Safety Builder shows the progress and the status of the compilation process on screen. All status messages displayed on screen are also logged in the log file.

Stop compiling

You can stop the compiler prematurely by pressing the **Abort** button during the compilation process.

This interruption of the compilation process is logged in the log file.

Controller file

The compiler creates a controller file when it has compiled the application successfully.

The controller file is stored in the same directory as the controller data, and is called "<controllername>.CCF".

Compiler registers and markers



Attention:

When you change, redraw, disconnect, relocate existing logic on FLDs or import entire FLDs, the embedded compiler markers and registers may be removed or regenerated, thus affecting the actual field states during an OLM.

Note that renumbering FLDs does not affect the field states during an OLM.

During an OLM the following should be considered:

- **All new or regenerated points on a modified FLD start with their power-up value.** This includes all regenerated compiler markers and registers and all imported and copied logic.
-

The compiler may introduce extra registers and markers in the application during compilation. These registers and markers store intermediate and feedback results so that they can be used in the application at a later stage. The names of these markers and registers always begin with the letter C of compiler.

Migrating applications

When installing a new or upgraded release of Safety Builder it is usually required to restructure existing plant and application databases in the Safety Station, before they can be accessed by the upgraded Safety Station.

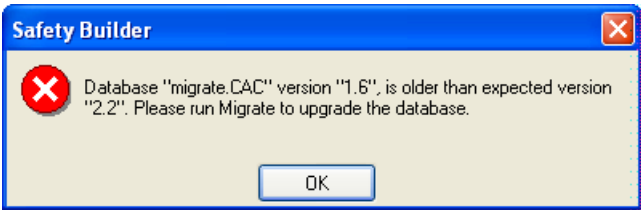
This necessary process step is called migration.



Note:
You do not need to compile and (re)load a migrated Safety Manager application, unless you want to upgrade the system as well.

Figure 37 on page 234 shows how Safety Builder prompts you when you open a plant that requires migration.

Figure 37 Plant migration is required.



This section covers the following topics:

| Section | See |
|----------------------------------|----------|
| Starting the Migrate Application | page 234 |
| Migrate Application menu | page 237 |

Starting the Migrate Application



- Notes:**
1. **Migrate Application** can only run after you started a plant configuration in Network Configurator.
 2. If you get a popup stating `exclusive access is denied` see “Working in a multi user environment” on page 236.
 - 3.

To start **Migrate Application**, you either:

- Open the tool via the menu bar (**Tools > Configuration > Migrate Application**)
- Press the shortcut keys **Alt, T, C, M**.

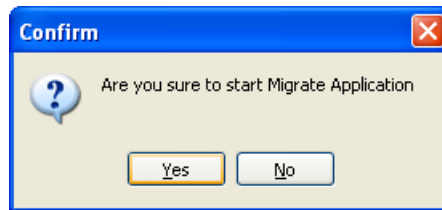
A pop-up screen as in Figure 38 on page 235 appears.



Stop:

Before you migrate to another release make sure you *check the release notes* to identify possible issues related to migration.

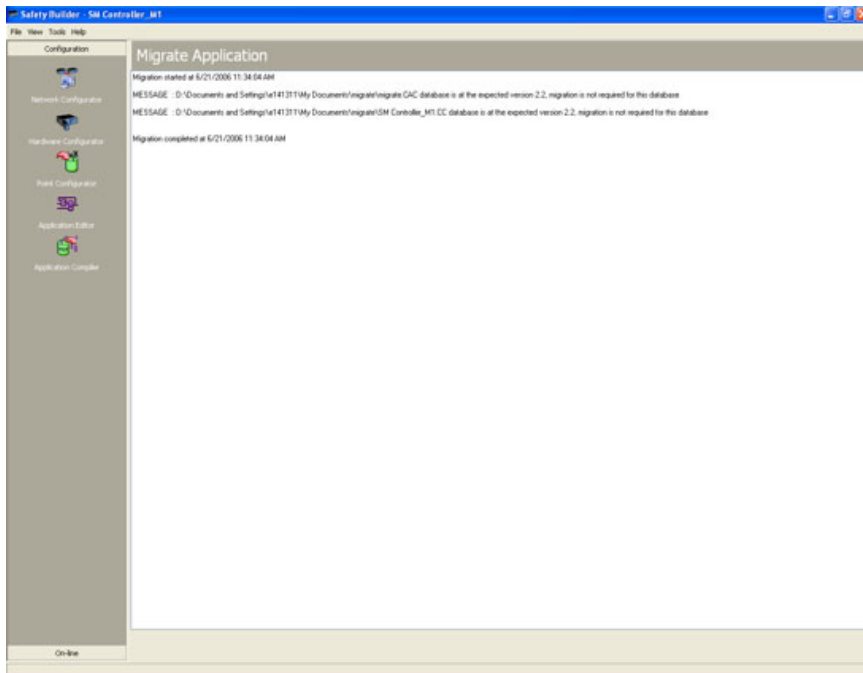
Figure 38 Starting the Migrate Application function.



The **Migrate Application** screen appears as shown in Figure 39 on page 236 and migration starts.

- The plant database <Plantname.CAC> is migrated first
- Next all SM Controllers <SM ControllerXY.CC> in the plant are migrated, including the diagnostic database files <SM ControllerXY.DGN>, if any.
- Each step of the migration progress is carefully logged, prompted on screen and stored in the application folder.
- If there is an error during the migration the entire plant will be restored and you must make the appropriate changes using the previous version of Safety Builder. (See the migration log file to determine which changes are required.)

Figure 39 Migrate Application screen



Working in a multi user environment



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
 2. To give up shared access exit the tool or function that demands shared access.
- To give up all access you can close the file (click **File>Close** from the menu bar).

When you try to access the Plant database with multiple users simultaneously, access to this tool may be limited or denied:

- If the Plant database is opened for shared use exclusive access to Network Configurator is denied and you get a popup stating:
Exclusive access is denied, please try again later.
- If the Plant database is opened exclusive use by some one else, access is denied and you get a popup stating:
Access is denied, please try again later.

In above cases, you cannot continue until the “denied access” lock is relieved by the other user(s).

For more information see also “Multi user environment” on page 36.

Migration log file

During the migration process, a log file is made. You can use the log file to analyze errors and, if necessary, deal with the warnings.

The log file is stored in the same directory as the controller/plant data, and is called `Migration report for <#name>.RTF`, where `<#name>` is the name of the controller or the plant that has been migrated.

To open the log file you must access this directory and double-click the `Migration report for...` files.

The log file is in RTF format.

Manual intervention when migrating

When migrating to a release with changed functionality the **Migrate Application** tool makes a best possible choice as how to change configuration settings to meet the new functionality.

This change is logged in the migration log file.

You need to verify that you agree with these changes and else modify the configuration changes made by **Migrate Application** before compiling.

Details of such changes (if any) can be found in the release notes and in the migration log file.

Migrate Application menu

Below list shows the Safety Builder **Migrate Application** menu structure.

The shortcut access key combinations, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also “Keyboard shortcut and access keys” on page 32.

| Menu item | Description |
|------------------------------|--|
| <i>File</i> | |
| > <i>C</i> lose | Closes Migrate Application. |
| > <i>E</i> xit | Exits Safety Builder. |
| <i>View</i> | |
| > <i>T</i> oolbars | Toggles display of the available toolbars. |
| > <i>O</i> utlook bar | Toggles display of the Outlook bar. |

| | |
|-------------------------------|--|
| > A udit Trail Viewer | Launches the Audit Trail Viewer. This option is shaded. |
| Tools | |
| > C onfiguration | Displays a sub menu with available configuration tools. For an overview see “Safety Builder configuration tools” on page 41. Unavailable tools will be shaded. |
| > O n-line | Displays a sub menu with available on-line tools. Unavailable tools will be shaded. |
| > P assword | Launches the Security tool (see “Security” on page 281). |
| > O ptions | Enables you to set general program options (see “Options” on page 274). |
| Help | |
| > S afety Builder help | Launches the Safety Builder Help function. |
| > A bout | Shows current version and license of the program. |

Safety Builder on-line tools

5

This section describes the various on-line tools available in the different Safety Builder packages.

With the on-line tools you can:

- load Controller files
- view diagnostics and system status data
- view application data and live FLDs



Tip:

Safety Builder can view live data in an online Safety Manager *even while the application version loaded in the system and in Safety Builder differ.*

For an overview of the tools available for each package, see “Safety Builder packages” on page 10.

| Tool | See |
|-----------------------|----------|
| Controller Management | page 240 |
| Application Viewer | page 261 |

Controller Management



Tip:
After migrating, modifying and compiling a running version of the application, Safety Builder can still view live data in an online Safety Manager *even while the application version loaded in the system and in Safety Builder differ.*

The Controller Management function in Safety Builder is an on-line tool that can perform the following:

- Show actual and historical diagnostic messages of Safety Manager.
- Store diagnostic messages from Safety Manager in a database.
- Display diagnostic messages on-line and off-line.
- Assist in resolving reported faults.
- Display Safety Manager on-line status information.
- Show the loop status of points of which a loop fault has been reported.
- Synchronize the Safety Manager time with the time of the Safety Station.
- Load a controller file into the Controller.

Most Controller Management functions require a connection between Safety Station and the relevant Safety Manager. This connection can either be direct or through the network.

This section covers the following topics:

| Section | See |
|-----------------------------------|----------|
| Starting Controller Management | page 241 |
| Controller Management menu | page 243 |
| Toolbars | page 245 |
| Component bar | page 245 |
| Using Controller Management | page 245 |
| Connecting to a Controller | page 246 |
| Diagnostic messages and databases | page 247 |
| Diagnostic tools | page 248 |
| Load Controller | page 251 |
| Status | page 253 |
| Time synchronization | page 260 |

Starting Controller Management

You can start Controller Management by:

- selecting **Tools > On-line > Controller Management** from the **Menu bar**,
- Clicking the **Controller Management** button in the on-line part of the **Outlook Bar**.
- Pressing the shortcut keys **Alt, T, N, A**.



Note:

If you get a popup stating `exclusive access is denied` see “Working in a multi user environment” on page 242.

If you start Controller Management, it will attempt to connect to the selected system.

- When successful a screen similar to Figure 40 on page 242 appears.
- Figure 41 on page 242 shows that you are prompted if Controller Management was unable to connect to the selected system.
 - If you click **OK** Controller Management will open with off-line functions only. For alternative methods to establish a connection with a Controller see “Connecting to a Controller” on page 246.
 - Clicking **Retry** will cause Controller Management to retry and establish a connection.
 - If you click **Abort** Controller Management will close.

Figure 40 Example of the Controller Management screen

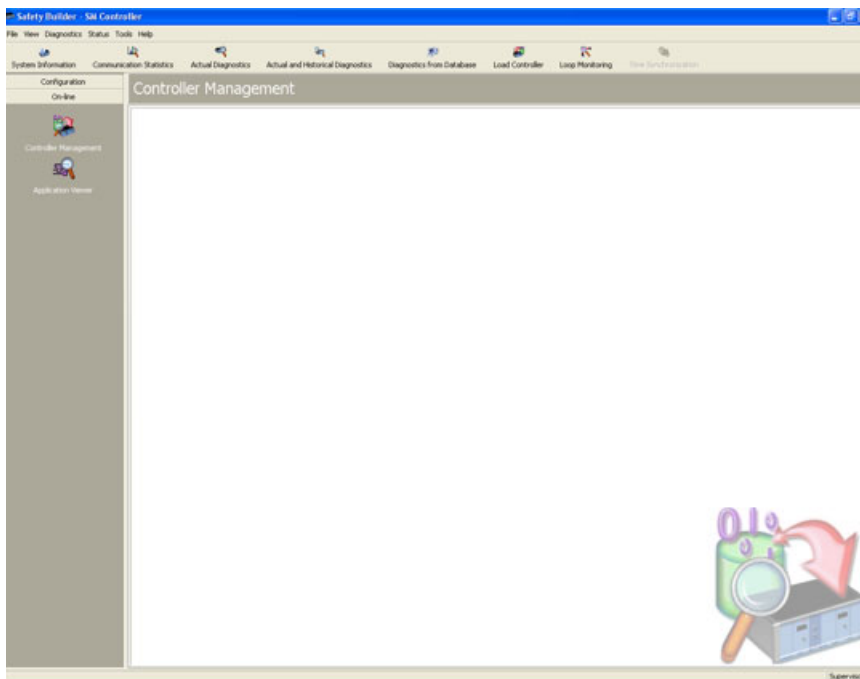
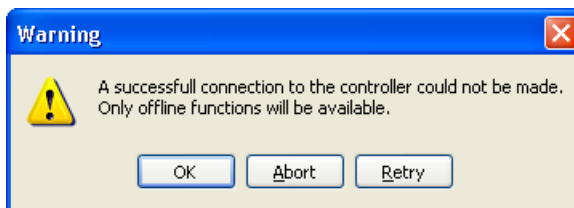


Figure 41 Controller Management warning display



Working in a multi user environment



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
 2. To give up exclusive access to an SM Controller access the **Network Configurator**.
 3. To give up shared access exit the tool or function that demands shared access.
- To give up all access you can close the file (click **File>Close** from the menu bar).

- When you try to access the SM Controller with multiple users simultaneously, access via this tool may be denied and you get a popup stating either:
- >**Audit Trail Viewer** Launches the Audit Trail Viewer (see "Audit Trail" on page 276).
 - >**Controllers** Access is denied. Opens a dialog in which a dialog that Controllers are listed so that a specific Controller can be chosen. Exclusive access is denied, please try again later. This option is only available after choosing **Load Controller** > **Load Controller**.
 - If the Plant database is opened for exclusive use by someone using Network Configurator, your access to this tool is denied.
- Diagnostics**
- If the SM Controller database is opened by someone, using this or a similar tool, your access to this tool is denied. Shows diagnostic messages since the last Fault Reset (see "Actual Diagnostics" on page 248).
 - >**Actual and Historical Diagnostics** In above cases, you cannot continue until the "denied access" lock is relieved by the other user(s). Shows all diagnostic messages since and before the last Fault Reset. (see "Actual and historical diagnostics" on page 249).
- For more information see also "Multi user environment" on page 36.

Controller Management menu

Below list shows the Safety Builder Controller Management menu structure.

The shortcut access key combinations, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also "Keyboard shortcut and access keys" on page 32.

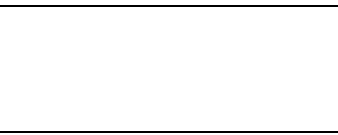
| Menu item | Description |
|-----------------------|-------------------------------------|
| File | |
| > C lose | Closes the Controller Management. |
| > E xit | Exits Safety Builder. |
| View | |
| > T oolbars | Toggles display of the toolbars. |
| > O utlook Bar | Toggles display of the Outlook bar. |

- >**Audit Trail Viewer** Launches the Audit Trail Viewer (see “Audit Trail” on page 276).
- >**Controllers** Opens a toolbar in which all connected Controllers are listed so that a specific Controller can be chosen

This option is only available after choosing **Load Controller > Load Controller**.

Diagnostics

- >**Actual Diagnostics** Shows diagnostic messages since the last Fault Reset (see “Actual Diagnostics” on page 248).
- >**Actual and Historical Diagnostics** Shows all diagnostic messages since and before the last Fault Reset. (see “Actual and historical diagnostics” on page 249)



- >**Safety Builder Help** Launches the Safety Builder Help function.
- >**About** Shows the version and license of Safety Builder.

Some of the Controller Management functions are also accessible through the toolbar of Safety Builder.

Toolbars



Note:

A toolbar only shows the most used tool functions and components. Some tool functions and components have to be accessed via an item in the Menu bar.

A toolbar contains a subset of tools or components that can be used by the active program.

Multiple toolbars can be active at the same time.

Controller Management

The **Controller Management** toolbar contains the most common functions of Controller Management.

Click **View>toolbars>Controller Management** to toggle the Controller Management toolbar.

Component bar

The **Component bar** is an Explorer bar as defined in “Explorer bar” on page 30. It shows an overview of the Components that can be selected.

The **Component bar**:

- highlights the component you have selected,
- provides you access to the connect/disconnect options, by right clicking a component. (See “Connecting to a Controller” on page 246 for details.)
- lets you connect to another Controller (for details see “Connecting to a Controller” on page 246.)

Using Controller Management

You use Controller Management to:

- Connect to a Controller, see “Connecting to a Controller” on page 246.
- Read diagnostic messages, see “Diagnostic messages and databases” on page 247 and “Diagnostic tools” on page 248.
- Read the system status, see “Status” on page 253.

Controller Management shortcut keys

Besides the shortcut keys listed in “Keyboard shortcut and access keys” on page 32 there are no shortcut keys active in Controller Management.

Connecting to a Controller

Once inside Controller Management you may want to select another Controller or (re)connect to an existing Controller.

To select a Controller:

- 1 Click the **Load Controller** button on the Toolbar. This will cause the **Component bar** to open and show a list of available Controllers.
- 2 To connect to a Controller, right-click the Controller in the **Component bar** that you want to connect to.
- 3 Select one of the available options, described below.

Connection options



Note:

In order to communicate with an SM Controller connection properties and configured system number must match between SM Controller and Safety Builder.

Connect

Connect will attempt to connect the Safety Station to the selected SM Controller.

In order to be able to connect:

1. Connection properties and configured system number must match between SM Controller and the application in Safety Builder.
2. At least one configured link must be setup and operational (Safety Builder will automatically try alternative links if the default link is down).

Temporary connect

Temporary connect is to be used to reload an SM Controller whose actual configuration is not matching the connection properties and/or system number as defined in the Safety Builder application.



Attention:

1. The temporary connect procedure in the *Installation and Upgrade Guide* requires you to erase the existing application from the SM Controller.
 2. Before loading an SM Controller with **Temporary connect**, disconnect all standard communication cables that are wired to the channel you use for temporary connect.
-

In order to connect with a SM Controller using **Temporary connect** certain conditions have to be met:

1. A serial connection to channel C of the SM Controller must be setup; Temporary connect does not work via Ethernet.
2. The SM Controller must boot with a default (empty) application.

The procedure to load using **Temporary connect** is described in the *Installation and Upgrade Guide*.

Disconnect

Disconnect will terminate the connection to the selected SM Controller.

Diagnostic messages and databases



Caution:

Turning the Reset key switch on the BKM will dump the diagnostic messages from the Actual diagnostics database into the Historical diagnostics database.

Safety Manager contains 3 diagnostic databases; 2 are located in the SM Controller, the third is located on the Safety Station.

1. **Actual diagnostics** is a database *located in the SM Controller* that only contains new diagnostic messages -these are all messages generated since the last time the Reset key switch was turned.
2. **Historical diagnostics** is a database *located in the SM Controller* that stores the last 320 historical messages dumped. It does not contain new diagnostic messages.

3. **Diagnostics database** is the database *located on disk in the Safety Station*; it contains all diagnostics that were loaded in the Safety Station. The diagnostics database can be accessed off-line.

A list of diagnostic messages can be found in “Diagnostic messages” on page 461.

Diagnostic tools



Attention:

1. Depending on your **Automatic Update** settings in **Tools>Options** a **Refresh** button may be visible to update the information on screen.
 2. If there are no diagnostic messages to report, the screen will display `No faults detected`, as shown in Figure 43 on page 250.
 3. If loop faults are detected *only the first* loop fault is logged in the diagnostic database with either the message `Open loop(s)` or `Analog input loop fault(s)`. Upon seeing either message you should check **Loop Monitoring** to see if more loop faults are detected. For more information see “Loop Monitoring” on page 251.
 4. Safety Station must be connected with Safety Manager to view the actual diagnostics
-

The following diagnostic tools are available in Controller Management to view the diagnostic messages from Safety Manager:

1. “Actual Diagnostics” on page 248
2. “Actual and historical diagnostics” on page 249
3. “Diagnostics from database” on page 249
4. “Loop Monitoring” on page 251

“Diagnostics database size” on page 250 explains how to change the diagnostic database size on the Safety Station.

Actual Diagnostics

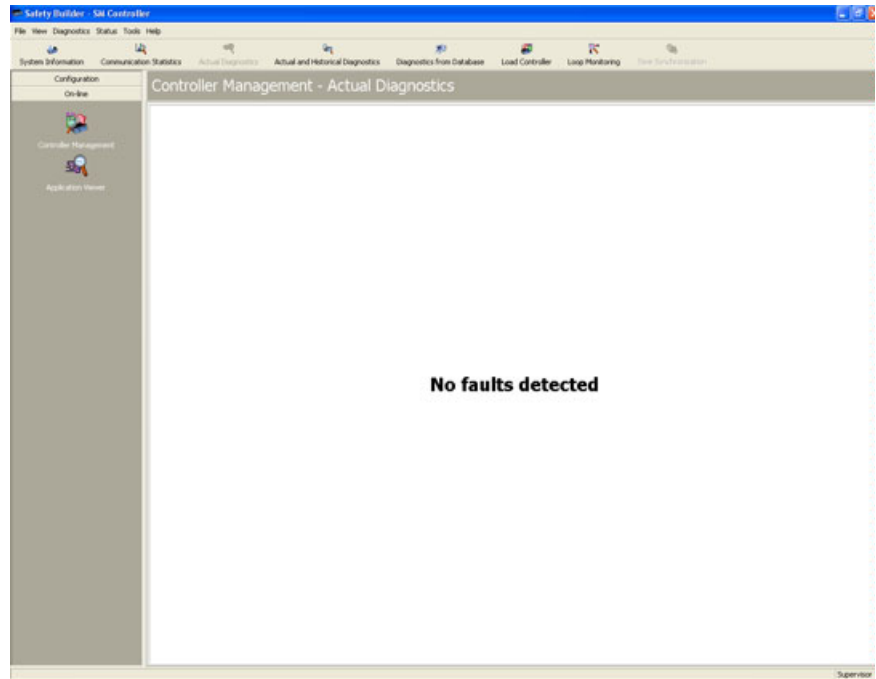
This option displays a window containing all diagnostic messages generated since the Reset key switch was last turned.

Controller Management retrieves these messages from the selected Safety Manager and stores them in the Diagnostics database for later reference.

Figure 42 on page 249 shows an example of **Actual Diagnostics**.

- The upper part of the screen shows a list of all actual diagnostic messages.
- The lower part of the screen displays any additional information about the diagnostic message that is selected in the upper part.

Figure 42 Actual Diagnostics screen



Actual and historical diagnostics

This option works in a similar way as the **Actual Diagnostics** screen but it *also* displays the historical diagnostic messages as stored on the Safety Manager.

When available on the Safety Station, Controller Management also displays the diagnostics from database.

Diagnostics from database

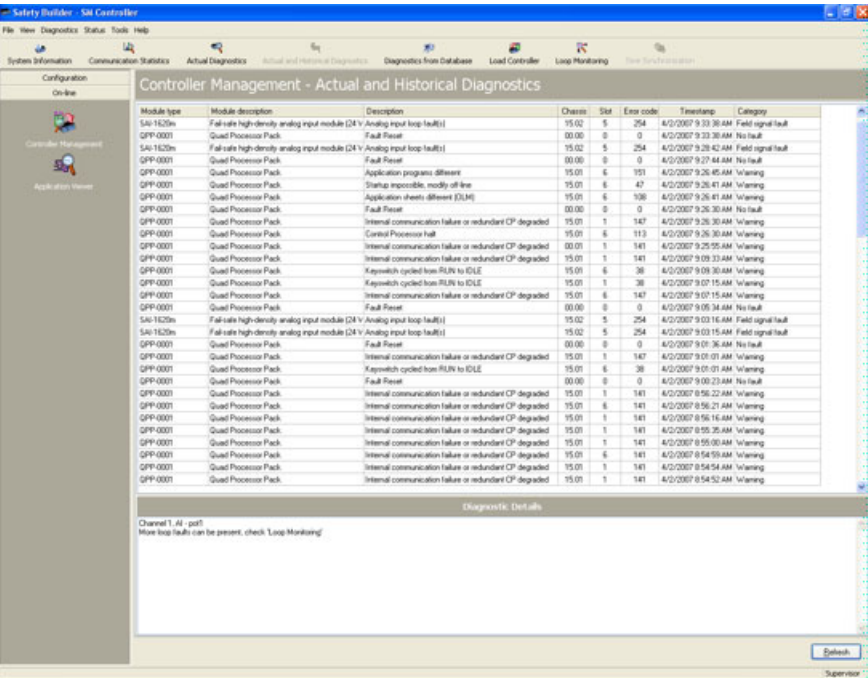


Attention:

The diagnostics database on the Safety Station is only updated by accessing the **Actual diagnostics** or **Actual and historical diagnostics** tools.

This option works in a similar way as the **Actual Diagnostics** screen but instead of showing diagnostic messages on-line, it displays diagnostic messages off-line via the diagnostics database on the Safety Station.

Figure 43 Diagnostics from Database screen



Diagnostics database size

This function enables you to change the maximum database size for diagnostic messages stored on the Safety Station.

The database uses a first-in-first-out system for storing diagnostic messages which means, if the maximum database size is reached, the oldest message is flushed on receipt of a new message. By increasing the database size, more diagnostic messages can be stored in the database.

Any database size between 1 and 100 MB can be chosen.

Loop Monitoring

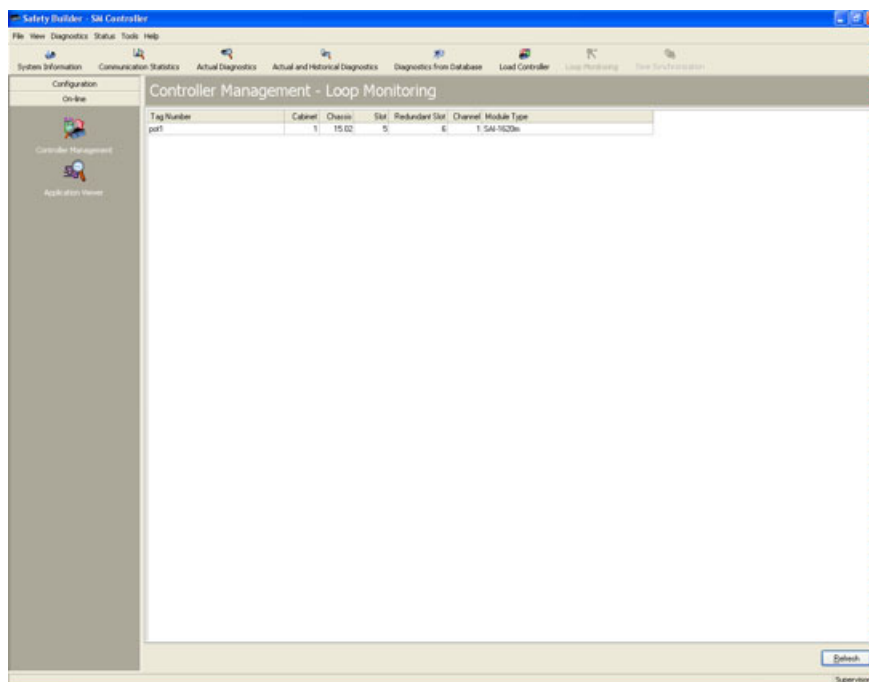


Notes:

1. **Loop Monitoring** can only be selected when the SM Controller is in Loaded mode (for details see “Controller status” on page 24.)
2. If loop faults are detected *only the first* loop fault is logged in the diagnostic database, all (subsequent) loop faults can be seen via the Loop Monitoring screen.
3. In addition either message `Open loop(s)` or `Analog input loop fault(s)` is reported: `Open loop(s)` is reported for line monitored digital IO loop faults, `Analog input loop fault(s)` is reported for analog input loop faults.

This screen shows the points of which a loop fault has been reported. It retrieves these loop fault messages from the selected Safety Manager.

Figure 44 Loop Monitoring screen



Load Controller

The **Load Controller** function enables the loading of the SM Controller file in the Control Processor(s).

Only persons authorized by Safety Builder can access this function. If a person is not authorized or the password has expired after a period of inactivity, Safety Builder automatically disables the access to this function (see also “Security” on page 281).

The content of this screen is interactive and by following the instructions on the display, you can load or restore the application in the Control Processors of the selected Safety Manager.

Load Controller screen



Tip:

After loading has been completed successfully the Controller status changes to loaded. See “Controller status” on page 24.



Attention:

If you load a Controller due to:

- **on-line modification**, you should follow the instructions as laid down in the *On-line Modification Guide*.
 - **off-line modification**, you should follow the instructions as laid down in the *Installation and Upgrade Guide*.
-

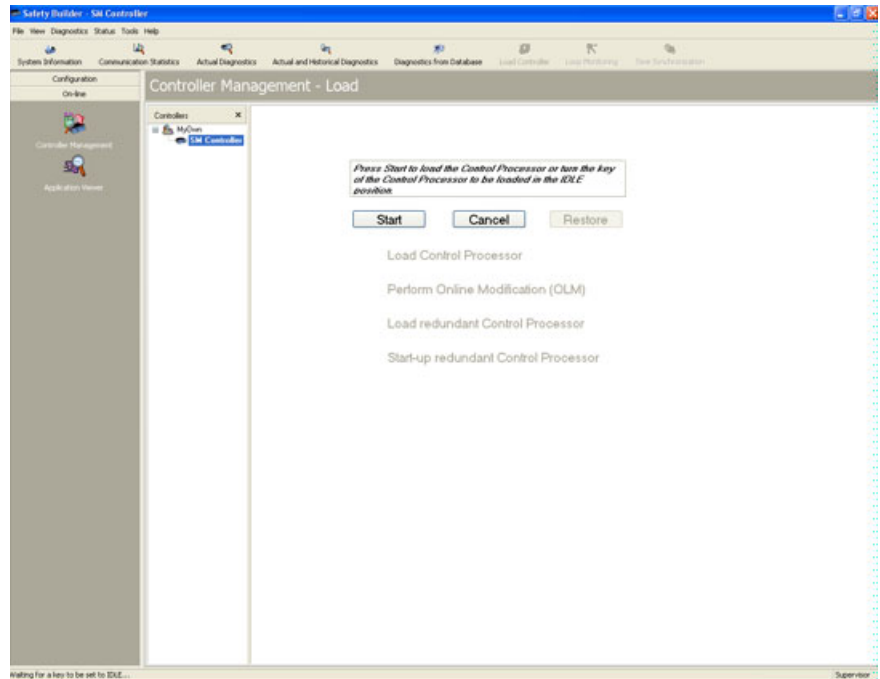
Figure 45 on page 253 shows the screen you get after clicking the **Load Controller** button from the Toolbar.

- Left of the workarea you see the **Component bar** where you can select the system you want to load.
- In the workarea four locations can be distinguished:
 - a. **The instruction bar:**
This area above the buttons is used by Load Controller to provide instructions to the user when stepping through the loading process.
 - b. **The buttons:**
Use the 3 buttons **Start**, **Cancel** and **Restore** to start or cancel the loading process, or restore the application. When shaded, the button is temporarily not available.
 - c. **The Status area:**
This area indicates which phases of the load process are in progress, completed or failed.
Status details of each phase can be found in the **Status bar** at the bottom of the screen.

d. **The Progress bar:**

This area at the bottom of the screen shows the current action.

Figure 45 Load Controller screen



Status

This section contains options to monitor the system status.

System information

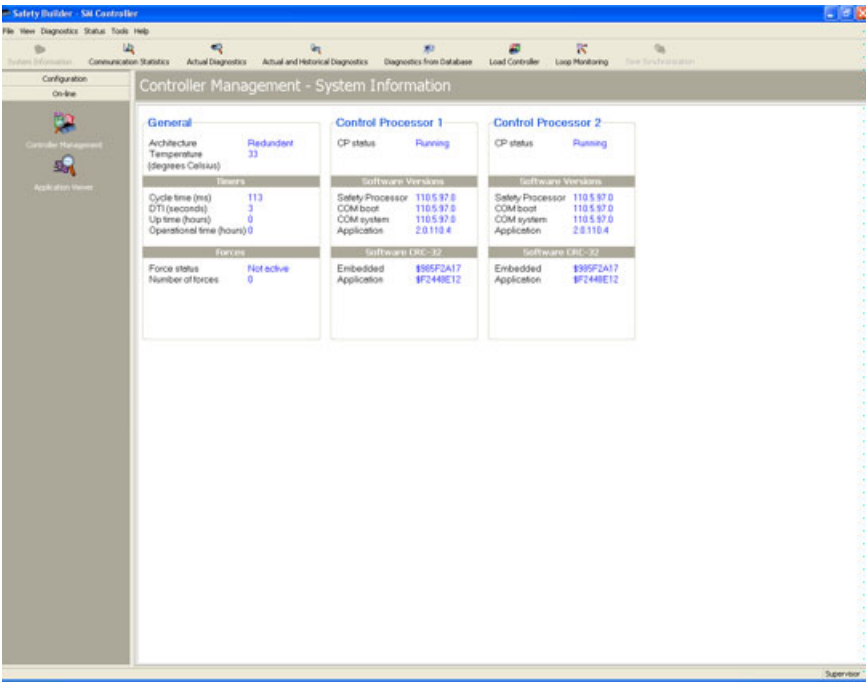
Controller Management has a **System Information** function with which Safety Builder can display various details about the selected Safety Manager and its Control Processor unit(s).

Figure 46 on page 254 shows the static and dynamic details as available from the **System information** window.



- Tip:
1. Some details, such as repair time, are only visible when they are in effect. For details see Figure 46 on page 254.
 2. If the software CRC-32 reports 0 or -1 for the embedded software, the embedded software is corrupted and needs to be reloaded.
In such cases you have also been prompted by the load function.

Figure 46 System Information screen



General information

The following general information is available:

General

- | | |
|---------------------|--|
| Architecture | Displays the SM Controller architecture |
| Temperature | Shows the SM Controller operating temperature. |

Timers

- | | |
|-------------------|---|
| Cycle time | Indicates the average application cycle time. |
|-------------------|---|

| | |
|-------------------------|---|
| DTI | Indicates the Diagnostic Test Interval; the time period available to locate and isolate safety related faults within on-line system components. |
| Up time | Indicates the time that the controller is powered up. |
| Operational time | Indicates how long the application has been running without interruption. |
| <i>Forces</i> | |
| Force status | If this status is Active points may be forced, if you have the appropriate privilege level. |
| Number of forces | Indicates the number of forced points. |

Control Processor information

For each Control Processor the following Control Processor information is available:

Control Processor X

| | |
|------------------|--|
| CP status | Indicates the CP status. For details see Table 44 on page 460. |
|------------------|--|

Software Versions

| | |
|-------------------------|---|
| Safety Processor | Shows the software version number of the embedded QPP firmware. This should be identical for both CPs. |
| COM boot | Shows the software version number of the embedded boot firmware for the communication modules. This should be identical for both CPs. |
| COM system | Shows the software version number of the embedded system firmware for the communication modules. This should be identical for both CPs. |
| Appl. version | Shows the software version number of the current application. |

Software CRC-32

| | |
|--------------------|--|
| Embedded | Shows the CRC of the embedded firmware. This should be identical for both CPs. |
| Application | Shows the CRC of the current application. This should be identical for both CPs. |

| | |
|----------------------------|--|
| <i>Repair Timer</i> | <i>Only visible when the repair timer is active.</i> |
|----------------------------|--|

| | |
|----------------|---|
| Actual | Shows the remaining repair time before the CP will shut down. |
| Maximum | Shows the maximum available repair time. |

Communication Status

To display details about the SM Controller communication status you can open the **Communication Status** window in Controller Management.

Figure 47 on page 257 shows an overview of the **Communication Status** window in Controller Management.

Communication Status has the following status tabs:

- **Communication Statistics**
This tab provides a list of all physical communication links of Safety Manager.
The **Communication Statistics** tab lists the communication statistics available per physical communication channel.
- **Link Status Report**
This tab provides a list of all logical communication connections of Safety Manager, except SafeNet and NTP/PTP connections.
The **Link Status Report** tab lists the actual diagnostic information available to the logical connections of the SM Controller.

Figure 47 Communication Status

Safety Controller - SM Controller 1

File New Diagnostics Status Tools Help

System Information Communication Status Actual Diagnostics Actual and Historical Diagnostics Diagnostics from Database Load Controller Loop Monitoring Time Synchronization

Configuration

On-line

Controller Management - Communication Status

Communication Statistics | Job Status Report

| Module | IDP | CDD Port | Protocol | Interface | Response Timeout | Data Corruption Error | Procedure Error | Operation Error | Incomplete Pages | Status |
|---------|-----|----------|--------------------|-----------|------------------|-----------------------|-----------------|-----------------|------------------|--------|
| US-0001 | CPH | 1B | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 1C | Mofbus | R1405 | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 1D | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2A | NTP-Espioner | Ethernet | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2B | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2C | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2D | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2E | Tuning Buffer PC2K | Ethernet | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2F | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 1C | Mofbus | R1405 | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 1D | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2A | NTP-Espioner | Ethernet | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2B | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2C | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |
| US-0001 | CPH | 2D | Not used | Not used | 0 | 0 | 0 | 0 | 0 | 0 |

Communication Statistics – tab

Communication Statistics provides an overview with statistics concerning various parameters per physical communication channel.



Note:

Communication Statistics records all occurrences since startup of the SM Controller.

The following statistics are logged:

| | |
|-------------------------------|--|
| Module | Identifies the communication module, CP and communication channel these statistics apply on. |
| CP | |
| COM port | |
| Protocol | Identifies the communication protocols active on this physical communication channel. |
| Interface | Identifies the configured interface for this physical channel. |
| Response Timeouts | Identifies the number of low level requests. |
| Data corruption errors | Identifies the number of messages with data corruption. |
| Procedure Errors | Identifies the number of messages with procedure errors. |

| | |
|--------------------------|---|
| Operation Errors | Identifies the number of unsupported messages. |
| Incomplete Frames | Identifies the number of messages with incomplete frames. |
| Retries | Identifies the number of retries. |

Link Status Report – tab



Attention:

Communication inputs that have *and* an *activated* fault reaction state of Low, High or Fixed, *and* are updated via auto-repairing logical connections, are *not* returned to their normal operating states when a faulty logical connection returns to healthy!

- If the communication input has a fault reaction set to Freeze or Hold the input is returned to normal operating state as soon as communication is resumed*.
- If the communication input has a fault reaction set to High, Low or Fixed, a **fault reset** is required to get the input returned to normal operating state and set the logical connection to healthy.

For more information see “Fault reaction and fault recovery for communication inputs” on page 298.

* Except for SafeNet: Completely broken SafeNet links do not auto-repair; they require a fault reset to return their inputs to healthy.

Link Status Report provides additional information per logical connection. You usually check the **Link Status Report** for detailed information when a link fault has been reported via the diagnostics.

- The **Link Status Report** is updated every second in the period that it reports changes in logical connection states.
- A time stamp indicates the last update of the **Link Status Report**: A frequently changing time stamp is thus an indication for an instable logical connection.
 - Logical connections that have *Auto Repair* enabled are continuously tested, even when reported faulty. When a faulty link returns to healthy again, communication is restored and the **Link Status Report** is updated.
 - Logical connections that have *Auto Repair* disabled only return to Healthy when the link is re-established *and* a fault reset is given. A fault reset also causes the **Link Status Report** to be updated.
- *Status CPx* indicates if the link is still up and running (at least one CP reports Healthy) or whether the link is down (both CPs report Faulty).

The following statistics are logged:

| | |
|-----------------------|--|
| Module | The communication module, physical channel and protocol used for this logical connection |
| COM port | |
| Protocol | |
| Device Address | The device address used for this logical connection: When displaying --, device addresses are not applicable. |
| Auto Repair | Indicates the response in case the connection should restore: Logical connections that have auto repair enabled will automatically recover from connection failures*. |
| Status CP1 | The status of the link as reported by CP1 |
| Status CP2 | The status of the link as reported by CP2 |

* For more information see the Attention box at the beginning of this section.

Remote Reset

There are two ways of resetting your SM Controller:

- The reset key switch
- The Remote Reset button

The reset key switch

The Reset key switch on the SM Controller performs a reset action which results in *one of* the below mentioned actions:

- Clear the fault database (actual diagnostics)
- Attempt a restart of tripped or halted Control Processors.
- Initiate a switch-over during an OLM procedure.

It may therefore be required to turn the key switch *twice* before the system starts!

The Remote Reset button



Note:

You must have the appropriate privilege level to operate the **Remote Reset** button in Controller Management.

The **Remote Reset** button on the **Controller Management** button bar allows you to remotely reset the SM Controller you are connected to.

The **Remote Reset** button results in the following actions:

- Clear non safety related faults from the database (actual diagnostics)
These include:
 - loop faults, short circuit faults
 - device communication faults,
 - single SafeNet connection faults (if one link is healthy and the other faulty)
 - warnings and messages (e.g. temperature pre-alarm)
- Attempt a restart of tripped or halted Control Processors

Time synchronization



Note:

The time is displayed as local time conform the 24 hour principle.

With this function of the Controller Management the time of the selected Safety Manager can be set to the Safety Station time.

This function requires:

- that the Safety Station has **Clock Source Allowed** enabled. For details see “Safety Builder properties” on page 74.
- confirmation from the user before time synchronization actually takes place.

Application Viewer



Tip:

After migrating, modifying and compiling a running version of the application, Safety Builder can still view live data in an online Safety Manager *even while the application version loaded in the system and in Safety Builder differ.*

The Application Viewer function in Safety Builder can perform the following:

- View in an FLD the actual point and signal values of an on-line Control Processor unit of the selected Safety Manager.
- Force and remove forces of points which have this option enabled.
- Change (“write”) the value of points which have this option enabled.
- View the properties of points.
- Monitor the execution of function blocks.
- Use the first-up alarm functionality.

The Application Viewer requires an operational logical connection between Safety Station and the relevant Safety Manager.

This section covers the following topics:

| Section | See |
|---------------------------------|----------|
| Starting the Application Viewer | page 262 |
| Application Viewer menu | page 263 |
| Toolbars | page 264 |
| FLD bar | page 264 |
| Using Application Viewer | page 265 |
| Viewing FLDs on-line | page 265 |
| Forcing and writing points | page 268 |

Starting the Application Viewer

You can start Application Viewer by:

- Selecting **Tools > On-line > Application Viewer** from the **Menu bar**,
- Clicking the **Application Viewer** button in the on-line part of the **Outlook Bar**
- Pressing the shortcut keys **Alt, T, N, A**

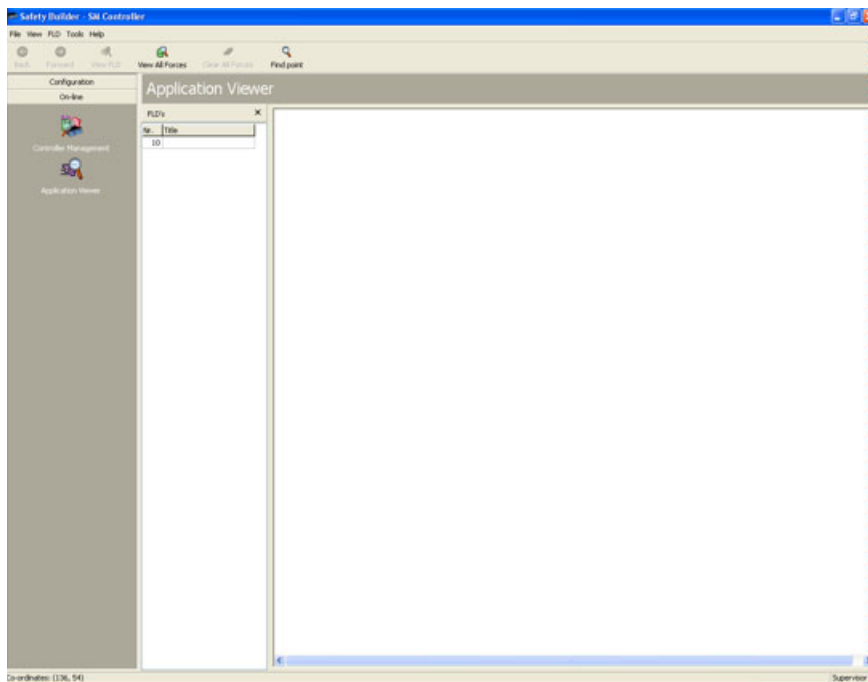


Note:

If you get a popup stating `exclusive access is denied` see “Working in a multi user environment” on page 263.

If you select Application Viewer in Safety Builder a screen similar to Figure 48 on page 262 appears.

Figure 48 Application Viewer screen



Working in a multi user environment



Tips:

1. To give up exclusive access to a Plant click **Stop Configuration** on the button bar.
 2. To give up exclusive access to an SM Controller access the **Network Configurator**.
 3. To give up shared access exit the tool or function that demands shared access.
- To give up all access you can close the file (click **File>Close** from the menu bar).

When you try to access the SM Controller with multiple users simultaneously, access via this tool may be denied and you get a popup stating either:

Access is denied, please try again later.

Exclusive access is denied, please try again later.

- If the Plant database is opened for exclusive use by someone using Network Configurator, your access to this tool is denied.
- If the SM Controller database is opened by someone, using this or a similar tool, your access to this tool is denied.

In above cases, you cannot continue until the “denied access” lock is relieved by the other user(s).

For more information see also “Multi user environment” on page 36.

Application Viewer menu

Below list shows the Safety Builder Application Viewer menu structure.

The shortcut access key combinations, to activate the menu items via the keyboard, are printed in bold face. For general information regarding shortcut keys, see also “Keyboard shortcut and access keys” on page 32.

File

- | | |
|-----------------|-----------------------------------|
| > C lose | Closes the Controller Management. |
| > E xit | Exits Safety Builder. |

View

- | | |
|------------------------------|--|
| > T oolbars | Toggles display of the toolbars. |
| > O utlook bar | Toggles display of the Outlook bar. |
| > A udit Trail Viewer | Launches the Audit Trail Viewer (see “Audit Trail” on page 276). |
| > F LD'S | Toggles display of the Explorer bar. |

| | |
|-----------------------------------|--|
| > B ack | Navigate back |
| > F orward | Navigate forward |
| > S caling | Allows you to scale the View FLD's window. |
| FLD | |
| <hr/> | |
| > V iew FLD | Opens the View FLDs window. |
| > V iew A ll Forces | Opens the View All Forces window. |
| > C lear All Forces | Clears all forces. |
| > F ind Point | Helps to locate a point in the Functional Logic Diagrams (FLDs). |
| Tools | |
| <hr/> | |
| > C onfiguration | Displays a sub menu with available configuration tools in Safety Builder. |
| > O n-line | Displays a sub menu with available on-line tools in Safety Builder. |
| > P assword | Launches the Security tool (see “Entering password” on page 282). |
| > O ptions | Enables you to set general Safety Builder options (see “Options” on page 274). |
| Help | |
| <hr/> | |
| > S afety Builder help | Launches the Safety Builder Help function. |
| > A bout | Shows the version and license of Safety Builder. |

Toolbars

Application Viewer

The **Application Viewer** toolbar contains the most common functions of Application Viewer.

Click **View>toolbars>Application Viewer** to toggle the **Application Viewer** toolbar.

FLD bar

The **FLD bar** is an Explorer bar as defined in “Explorer bar” on page 30.

The **FLD bar** lists the available FLDs of the selected Controller.

Selecting an FLD

To select an FLD from the **FLD bar** double click the FLD in the **FLD bar**.

Using Application Viewer

To use Application Viewer to:

- View on-line FLDs, see “Viewing FLDs on-line” on page 265.
- Force and write points, see “Forcing and writing points” on page 268.

Application Viewer shortcut keys

Besides the shortcut keys listed in “Keyboard shortcut and access keys” on page 32, the following shortcut keys are active when you use the Application Viewer:

- Pressing the **PageUp** or **PageDown** key will scroll one FLD up or down.
- Pressing **CTRL+A** will open a view with a list of all forces
- Pressing **CTRL+D** will open the **View FLDs** window
- Pressing **CTRL+F** will open the **Find Point** window

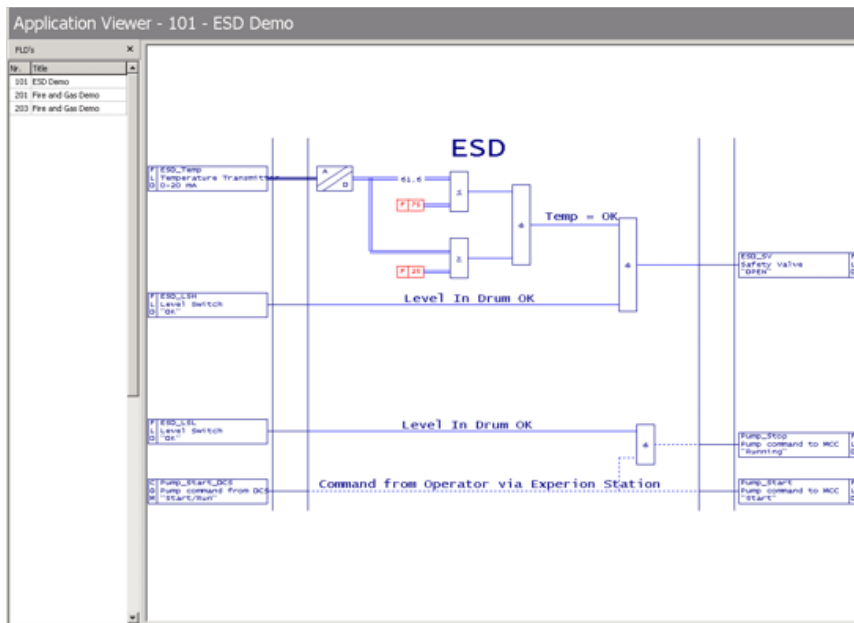
Viewing FLDs on-line

Figure 49 on page 266 shows an example of viewing FLDs on-line.

Viewing FLDs on-line is almost identical to viewing FLDs in the Application Editor (see “Application Editor” on page 178). You can navigate through the pages in the same way. The difference is that you cannot change the drawing but can view the on-line values of points and signals of a Control Processor unit of the selected Safety Manager.

Depending on the options set in the Point Configurator (see “Point Configurator” on page 141), points can be forced and values can be written.

Figure 49 Example of an FLD viewed online



Navigating through FLDs




Several options are available to navigate through FLDs once you have an FLD open.

If you:

- press the **PageUp** or **PageDown** key on your keyboard you will scroll one FLD up or down.
- double-click an onsheet or offsheet reference in an FLD you jump to the FLD that the sheet reference points to.
- double-click a Function Block in an FLD you jump to the Function Block FLD.
- use the **Find Point** option you jump to the FLD the point is used on.
- double-click another FLD in the **FLD bar**, that FLD will open.
- click the **Back** or **Forward** button in the **Go to** toolbar you can browse the history of viewed FLDs.

Information in the display

In an on-line viewed FLD the values of points and signals are presented as follows:

| Value | Presentation |
|--|---|
| Binary The current application value of a binary -or numeric- signal is stated in the double line of the signal. |  |
| Boolean The current state of boolean -or logic- signals is represented by the line format: <ul style="list-style-type: none"> • A continuous line represents a High, 1 or On state • A dashed line represents a Low, 0 or Off state. |  |
| Timer, counter and register The current value of counters, timers and registers is stated inside the symbol. |  |



Note

You cannot view the on-line values in a function block FLD since it can be used in several FLDs. However you can view the input and output signal values of a function block by going to the FLD in which it is used.

Viewing FLDs and finding points

For navigating through the FLDs and finding points see “Application Editor” on page 178.

When viewing an FLD on-line you can influence the displayed values if the appropriate options have been set in the Point Configurator (see “Point Configurator” on page 141). These changes immediately affect the operation the selected Safety Manager since they are carried out in the Control Processor.

Point properties

You can inspect the properties of a point in an on-line viewed FLD by:

- right-clicking its symbol and then selecting **Properties**.
- Double clicking the point

In both cases a **Point properties** window pops up. This window is view only.

Application cannot be viewed

If you are viewing FLDs online and the text Application data cannot be viewed is displayed in the work area, Safety Builder is unable to retrieve live application data from the Controller. In response the **Application Viewer** work area and **FLD bar** will blank.

Safety Builder is unable to retrieve live application data from the Controller if:

- Loss of communication with the Controller
- The applications in Safety Builder and Controller do not match (anymore)
- The application is brought off-line, e.g. due to a halted Controller.

Forcing and writing points

View all forces

To get a list of applied forces you can:

- click the **View All Forces** button from the **Toolbar**,
- click **FLD>View All Forces** from the menu bar or
- type an **A** while holding down the **Ctrl** key.

If there are no forces active in the selected Controller the window message will say so.



Tip:

If you double-click a point in the **View All forces** window Safety Builder will display the online FLD where the point is allocated.

The View all Forces window shows the following detail of the forced points:

- Point type
- Tag number
- Actual value (for inputs this is the field value, for outputs this is the value as displayed on the FLD going to the output)
- Force value
- Engineering units
- FLD where point is used

Forcing a point

**Stop:**

Forcing points can be dangerous if not handled properly! Always communicate your actions when applying or removing forces.

**Attention:**

To immediately remove *all* forces:

- turn the Force Enable key switch or
- click the **Remove All Forces** button on the **Application Viewer** toolbar.

Warning:

This action is irreversible.

In some occasions it may be necessary to force a point to a fixed state, for example when a defective input sensor needs to be exchanged. This allows you to perform maintenance on the Safety Manager without affecting the process continuity by forcing appropriate points, which have this option enabled, to their normal operational state.

All forcing operations are logged for traceability.

The following forcing operations are possible:

- Forcing of a digital point type (DI, DO, M) to low, high or clearing the force.
- Forcing of a float type point (AI, AO, BI, BO, R). The valid range equals that of a float: -1E38.. +1E38.
- Forcing of an integer type point (BI, BO, R, T, C). Ranges for BI, BO and R equal their corresponding integer type (8-, 16- or 32 bits signed). For T and C the range depends on the configuration. See Table 34 on page 400 for range specifications.
- Clearing the force on a selected point.

To force a point, select a point, right-click it and choose **Force**.

To clear a point, select a point, right-click it and choose **Clear**.

Writing a point

You can change the value of points which have this option enabled. The value remains in effect until it is updated by the Control Processor. You can only change the values of:

- digital COM inputs
- binary COM inputs
- markers
- registers
- counters
- running timers

To write a point, select a point, right-click it and choose **Write**.

Clear all forces



Warning:

This action is irreversible!

To immediately remove *all* forces:

- turn the Force Enable key switch or
- click the **Remove All Forces** button on the **Application Viewer** toolbar and confirm in the popup window.

Miscellaneous Safety Builder tools

6

This section describes the miscellaneous tools available in the different Safety Builder packages.

Miscellaneous tools are used to:


- apply user settings to Safety Builder and
- support the main configuration and on-line tools.

For an overview of the tools available for each package, see “Safety Builder packages” on page 10.

| Tool | See |
|---------------|----------|
| Find | page 272 |
| Configuration | page 274 |
| Audit Trail | page 276 |
| Security | page 281 |

Find

- In all configuration tools you have a find function.
- For large projects you can use the find function to easily locate components. You can access this function by:
- Selecting **Edit > Find** from the **Menu bar**,
 - Clicking the **Find** button from the **Toolbar** or
 - Pressing the shortcut keys **Ctrl+F**.



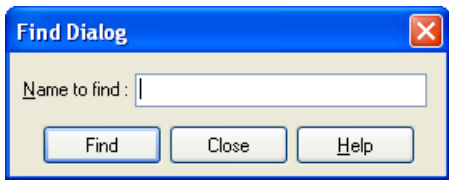
Tip:

- A search is case sensitive; searching for “test” will not find “Test”.
- Use the asterisk sign (*) as a wildcard; searching for “test*” will find “test” but also “test 1” and “test 2”.

Depending on the tool, the functions’ dialog window and options may vary.

For details see the references indicated below:

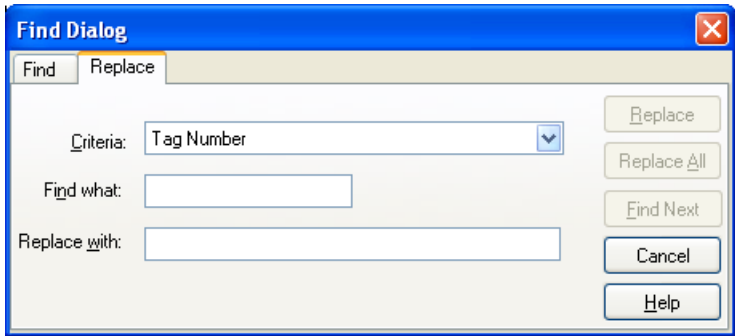
Find tool as displayed in Network Configurator and Hardware Configurator



For proper use of Find in Network Configurator see “Find Dialog” on page 67.

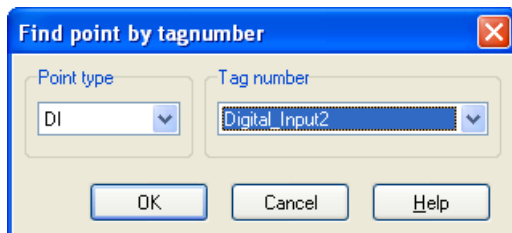
For proper use of Find in Hardware Configurator see “Find Dialog” on page 133.

Find tool as displayed in Point Configurator



For proper use of Find in Point Configurator see “Find Dialog” on page 164.

Find tool as displayed in Application Editor and Application Viewer



For proper use of Find in Application Editor and Application Viewer see “Finding points” on page 220.

Configuration

You can configure the layout of the interface to suit your personal preferences. The size of the interface and its components can be altered by dragging the outer and inner borders respectively.

To customize the interface, open the **View** menu and choose all interface elements you want to be displayed (toolbars, outlook bar).

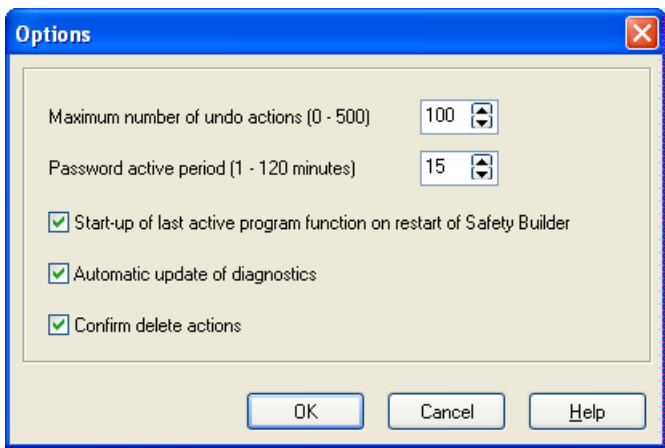
The size of the outlook bar icons can be changed by right-clicking in the outlook bar and choosing the size of your preference.

The interface configuration is automatically stored when you close Safety Builder.

Options

The **Options** window allows you to configure general Safety Builder settings. If you change any of these options, it will automatically be saved when you close Safety Builder.

You can access the options menu by selecting **Tools > Options**.



| | |
|--------------------------------|--|
| Maximum number of undo actions | This number defines how many actions are recorded for the undo function. For example, if you set this to three you can undo the three most recent changes. |
| Password active period | Password active period is the period that a password stays valid when no user interaction is recorded for Safety Builder. See also “Password active period” on page 284. |

| | |
|---|---|
| Start-up of last active program function on restart of Safety Builder | If enabled, Safety Builder automatically launches the last active program when started. |
| Automatic update of diagnostics | If enabled, Safety Builder will automatically update diagnostics on screen when Extended Diagnostics function is selected (see: “Controller Management” on page 240). |
| Confirm delete actions | If enabled, Safety Builder asks for confirmation before deleting actions. It is recommended to keep this option enabled. |

Audit Trail

Audit Trail logs, views and archives changes to Plants and Controllers.
Only the changes that affect the functionality of the safety instrumented functions are logged.

Changes to Plants and Controllers are logged as events.

- To see how events are logged, see “Event justification” on page 276.
- To view logged events, see “Audit Trail Viewers” on page 277.
- To view the kind of events logged, see “Event generating actions” on page 279.
- To see how events can be archived see “Archiving events” on page 279.



Tip:

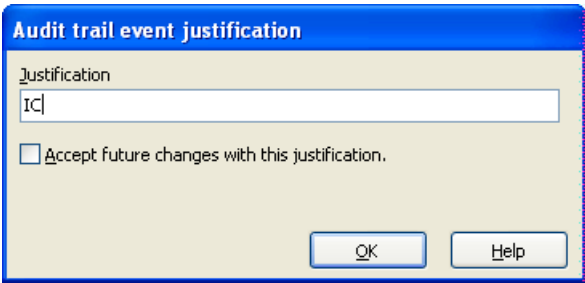
Archiving your Audit Trail events on a regular basis will improve Safety Builder performance. For details see “Archiving events” on page 279.

The Audit Trail functionality is always active when working in Safety Builder.

Event justification

When you execute an event generating action (see “Event generating actions” on page 279 for an overview), a window will appear asking you for an event justification. The window looks like Figure 50 on page 276.

Figure 50 Audit trail event justification window



In the **Justification** field you must enter the motive of the current action. The text entered here will appear in the Audit Trail Viewer for diagnostic purposes (see “Audit Trail Viewer windows” on page 277).

You can use the **Accept future changes with this justification** check box if you want that the changes you intend to make during this session are logged under the same justification without opening a new Audit trail event justification window. The current session ends when you go to another configuration screen of Safety Builder (for example when you go from Hardware Configurator to Network Configurator).

Audit Trail Viewers

You can use an Audit Trail Viewer to view and archive the events logged by Audit Trail.

An Audit Trail Viewer can be started by selecting **View > Audit Trail Viewer** from the menu bar. Depending on the Safety Builder tool that is active a specific Audit Trail Viewer is activated.

The following Audit Trail Viewers can be activated:

- Plant Audit Trail Viewer
- Controller Audit Trail Viewer

Plant Audit Trail Viewer

The Plant Audit Trail Viewer logs all changes made to the Plant configuration. You can only access the **Plant Audit Trail Viewer** from within Network Configurator.

To open the Plant Audit Trail Viewer select **View > Audit Trail Viewer** from the menu bar of the Network Configurator.

If this menu item is disabled, you will first need to start the Plant configuration.

Controller Audit Trail Viewer

The Controller Audit Trail Viewer logs all changes made to the Controller configuration. You can only access the **Controller Audit Trail Viewer** from within Network Configurator.

To open the Controller Audit Trail Viewer select **View > Audit Trail Viewer** from the menu bar of any tool *except the Network Configurator*.

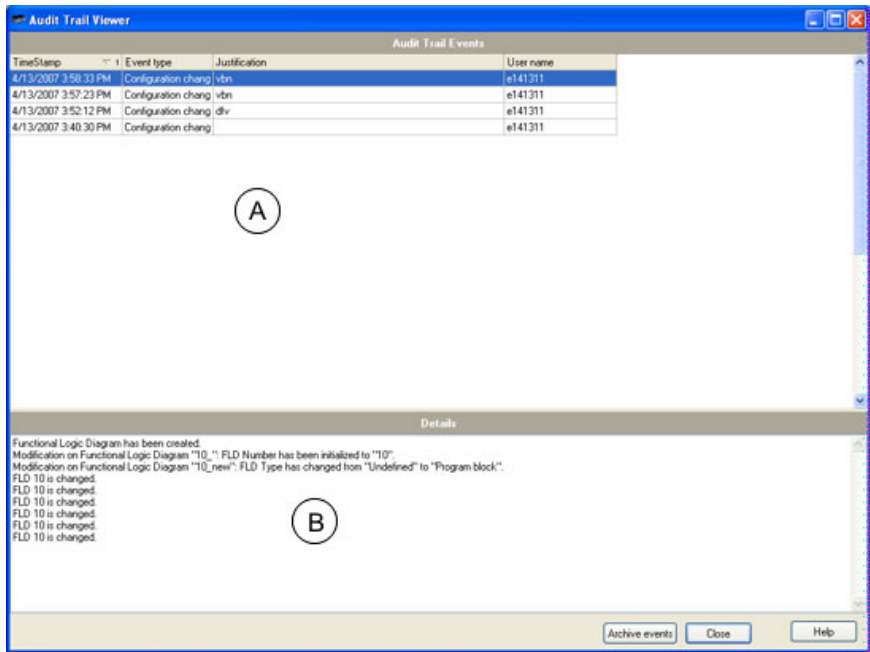
Audit Trail Viewer windows

All Audit Trail Viewers work the same: Only the events contained within them differ per type of Audit Trail Viewer.

Figure 51 on page 278 shows an example of an Audit Trail Viewer window. Each Audit Trail Viewer window has two sub-windows:

- 1. The Audit Trail Events window (section “A” in Figure 51 on page 278)
- 2. The Details window (section “B” in Figure 51 on page 278)

Figure 51 Audit Trail Viewer main screen



Audit Trail Events

The **Audit Trail Events** window displays the following properties:

- TimeStamp** contains the date and time of the event.
- Event type** contains the type of event that occurred.
- User name** the user that generated the event.
- Justification** the justification as entered by the user when the event occurred (see “Event justification” on page 276).

The items displayed in the **Audit Trail Events** list can be sorted on the contents of any of the columns by clicking on the heading of that column.

Details

You can select an event in the **Audit Trail Events** window by clicking it. The **Details** window will then display a detailed description of the selected event.

The following information is shown in the Details window:

- The object that was created, modified or deleted.
- The properties of the object that were changed.
- The value of the property before it got changed during the logged event.
- The value of the property after it got changed during the logged event.

Event generating actions

Table 9 on page 279 shows the actions that generate an Audit Trail entry.

Table 9 Actions that generate an Audit Trail entry

| Event type logged | Audit Trail Viewer | |
|---|--------------------|------------|
| | Plant | Controller |
| Changing the configuration of the Plant. | X | |
| Changing the Controller configuration. | | X |
| Changing the application program. | | X |
| Creating a controller file. | | X |
| Loading a controller file. | X | |
| Restoring the communication architecture and the application files. | | X |
| Activating/clearing Forces. | | X |
| Setting the Real Time Clock of the Controller. | | X |
| Executing Write commands. | | X |
| Occurrences of data and program integrity errors. | X | |



Note:

In some occasions it is possible that multiple changes are logged as a single entry. For example functional changes to a functional logic diagram in the Application Editor.

Archiving events



Tip:

Archiving events logged by the Audit Trail Viewers on a regular basis, e.g. once a week, will:

1. improve Safety Builder performance
2. speed up the archiving process.

When archiving, the Audit Trail Viewer Events are saved to a comma separated text file with extension CSV.



Notes:

1. Plant Audit Trail Viewer events and Controller Audit Trail Viewer events must be archived separately.
 2. If large archives are to be created the archiving process may take up several minutes or hours.
-

To move logged events to an archive file, do the following:

- 1 Open the Plant or Controller Audit Trail Viewer (see “Audit Trail Viewers” on page 277 for details).
- 2 Sort the events on their timestamp by clicking on the **TimeStamp** column heading.
- 3 Select the latest event that you want to include in the archive:
The selected event, including all older events, will be archived and removed from the Audit Trail database.
- 4 Click **Archive events**.
- 5 In the Archive Audit trail events window, click **OK** to start archiving.
- 6 Enter a name and location for the archive file, and click **Save**.

All archived events are removed from the Audit Trail database, so they are not displayed anymore in the Audit Trail Events window, and they are saved to the .CSV file you selected.

Security

Safety Builder has security features which prevent unauthorized access to the following Safety Builder functions:

- Forcing variables
- Writing variables
- Loading applications
- Application configuration

The security features are invoked by password protection. Password protection allows an unauthorized user to view information but not to make modifications.

In Safety Builder, the following users and privileges can be defined:

Table 10 Privileges for different users in Safety Builder

| Privileges | Active user | | | | | |
|--|-------------|-------------|---------|-------------|----------|-----------|
| | Supervisor | Engineering | Loading | Maintenance | Operator | View Only |
| Password configuration | yes | | | | | |
| Archive Audit Trail events | yes | | | | | |
| Full access to Network Configurator, excl. password config. | yes | yes | | | | |
| Full access to Hardware Configurator | yes | yes | | | | |
| Full access to Point Configurator | yes | yes | | | | |
| Full access to Application Editor | yes | yes | | | | |
| Full access to Application Compiler | yes | yes | | | | |
| Full access to Restore Configuration | yes | yes | | | | |
| Full access to Rebuild Safety Manager database | yes | yes | | | | |
| Full access to Safety Checker | yes | yes | | | | |
| Full access to Application Verifier | yes | yes | | | | |
| Full access to Availability Checker | yes | yes | | | | |
| Import/Export Point database | yes | yes | | | | |
| Load Controller, including OLM | yes | | yes | | | |
| Retrieve Controller and Application files | yes | yes | yes | | | |
| If a password protected privilege level is left unattended for a period of time, the privilege level changes to <i>the highest available level without password protection</i> . | | | | | | |
| The "View only" level has no password protection. | | | | | | |

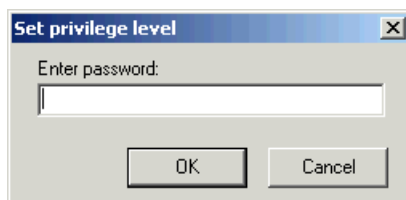
Table 10 Privileges for different users in Safety Builder (continued)

| Privileges | Active user | | | | | |
|---|-------------|-------------|---------|-------------|----------|-----------|
| | Supervisor | Engineering | Loading | Maintenance | Operator | View Only |
| Enable “remote” load | yes | yes | yes | | | |
| Set controller loaded | yes | yes | | | | |
| Forcing Points | yes | | yes | yes | | |
| Retrieve Actual Diagnostics | yes | yes | yes | yes | yes | yes |
| Retrieve Actual and Historical Diagnostics | yes | yes | yes | yes | yes | yes |
| Set Safety Manager time synchronization | yes | | yes | yes | | |
| Writing Points, such as set points with location “COM” | yes | | yes | yes | yes | |
| View System Status | yes | yes | yes | yes | yes | yes |
| View Loop Monitoring | yes | yes | yes | yes | yes | yes |
| View Application | yes | yes | yes | yes | yes | yes |
| View Points | yes | yes | yes | yes | yes | yes |
| View Network Configuration | yes | yes | yes | yes | yes | yes |
| View Hardware Configuration | yes | yes | yes | yes | yes | yes |
| View Point Configuration | yes | yes | yes | yes | yes | yes |
| View Audit Trail | yes | yes | yes | yes | yes | yes |
| If a password protected privilege level is left unattended for a period of time, the privilege level changes to <i>the highest available level without password protection</i> . The “View only” level has no password protection. | | | | | | |

Entering password

You can access the password window by selecting **Tools > Password** or by double-clicking the passwords section of the status bar (bottom-right). Note that this is only possible after you have chosen **Start Configuration** earlier.

If you do so, the **Set privilege window** appears:



When you enter your password, each valid key stroke is reproduced on screen as an asterisk ('*'). Typing errors can be corrected with the [BACKSPACE] key. The password protection feature is automatically activated when Safety Builder is not used for a certain period of time.

Safety Builder has a supervisor function for setting or changing passwords for particular functions. The supervisor can also set the inactivity period, after which the granted access is revoked.



Note:
You do not need any password to view configuration data of Safety Builder.

Changing passwords

You can change the password for every available security level. To access the **Change Password** window select **File > Change Password**. Note that this is only possible after you have chosen **Start Configuration** earlier.

If you do, a window similar to the following appears.

Privilege Level Select the security level of which you want to change the password.

New password Enter the new password for the selected user.
Leaving this text box empty will remove the password for the selected user.

Confirm password Enter the new password for the selected user again for confirmation.
Leaving this text box empty will remove the password for the selected user.

Changing passwords is only possible when you are logged in as supervisor.



Attention:

To protect a level with a password, you must also protect the higher levels with a password, as Safety Builder jumps to a highest available level without password protection in case of a time-out!



Note:

For maximum security, it is advised to change passwords frequently.

Password active period

The Password active period is the amount of time a password remains valid when no user interaction is recorded for Safety Builder. This means that if you do not use Safety Builder for this period, the security level automatically switches to the *highest available* level without password protection. You then need to re-enter a password to revert to the prior security level.

You set the password active period in the **Tools > Options** menu.

Forgotten supervisor password

If you forget or somehow lose your supervisor password, you are no longer able to change Safety Builder passwords. You then need to contact Honeywell SMS to request a resetting of the supervisor password.

Communication

A

APPENDIX

This appendix provides background information with respect to communication and time synchronization topics.

The following topics are discussed in this appendix:

| Topic | See |
|---|----------|
| Communication options | page 286 |
| Communication via the Experion protocol | page 299 |
| Communication via the Peer Control Data Interface | page 303 |
| Communication via the Modbus protocol | page 309 |
| Communication via the SafeNet protocol | page 318 |
| Communication via the Safety Builder protocol | page 329 |
| Real-time clock synchronization | page 332 |

Communication options

Process control and safeguarding functions in today's process industry are highly automated via computerized systems. One advantage of computerization is the possibility of gathering and exchanging digitized information of process parameters.

In order to make optimal use of this information and to be able to provide adequate information to plant operators, both the process control systems and the safeguarding systems must have communication capabilities to exchange process information.

Safety Manager can communicate with the following devices:

- Experion™ servers
- Experion CEE controllers
- MODBUS RTU and Modbus TCP devices
- Other Safety Managers
- Safety Station
- PTP and NTP based clocks

Network components

Network master

A network master is a device component in the network (such as a Safety Manager, a Modbus device, a CEE controller etc.) that initiates, and controls, communication sessions with slave systems.

- A network (e.g. SafeNet or Modbus) may have multiple masters per network layer;
- a SafeNet network master can connect to up to 62 slaves;
- A SafeNet network master can also be configured as a network slave to other masters in the same network layer or in adjacent network layers;
- A SafeNet network master has the ability to reset slave systems.

Network slave

A network slave is a system in the network that responds to a communication initiative from network masters, such as another Safety Manager, a Modbus device, a CEE controller etc.

- A network slave may be connected to several masters and to several networks;
 - A SafeNet slave may be connected to up to 62 masters per SM Controller;
 - A Modbus slave may be connected to up to 8 Modbus masters per Ethernet channel (plus one per serial channel);
- A SafeNet network slave may also be configured as a network master for communication to other slaves in the same network layer or in adjacent network layers.

Link types

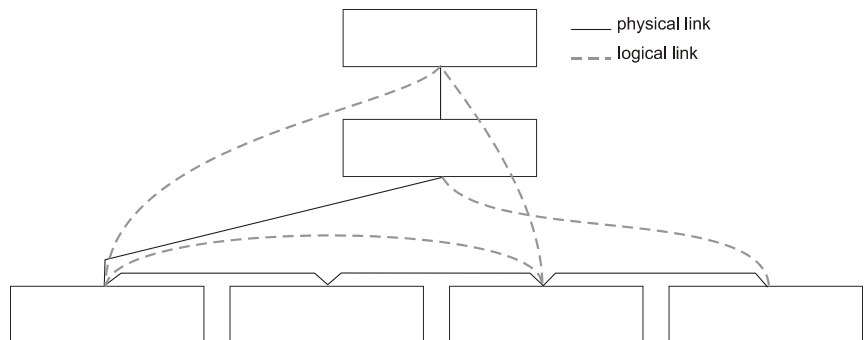
Physical and logical links

You can view links in two ways:

- From a logical (data exchange) point of view
- From a physical (cabling) point of view

Figure 52 on page 287 shows how Safety Manager distinguishes between physical links and logical links.

Figure 52 Physical and logical links



Physical and logical link views are equally important but differ in functionality:

- A logical link forms a virtual connection between two systems that exchange data.
 - Time-outs and response times are based on the amount of data assigned to the logical link
 - Logical links can be defined between a master and a slave, and between two SM Controllers acting as slave peers (in which case one slave becomes the master of the other)

- A logical SafeNet link may span up to 7 physical links

The dashed connection lines in Figure 52 on page 287 provide examples of logical links.

- The physical link includes all components required to create the physical connection of systems within the network.
 - Physical links determine the transport protocol(s) used and communication speed of that (those) link(s).
 - Multiple logical links can be realized across a physical link.
 - Multiple physical links can be used to realize a logical link.

Point to point link



Notes:

- A point to point link can also be referred to as a peer-to-peer link.
- Logical links are always point to point!

Figure 53 on page 288 shows that a point to point link is a link that connects two systems together; there are no other devices connected on the same communication link.

Point to point links can be logical or physical.

Figure 53 Point to point link



Multidrop link



Note:

Multidrop links are only supported with Ethernet or RS485 links.

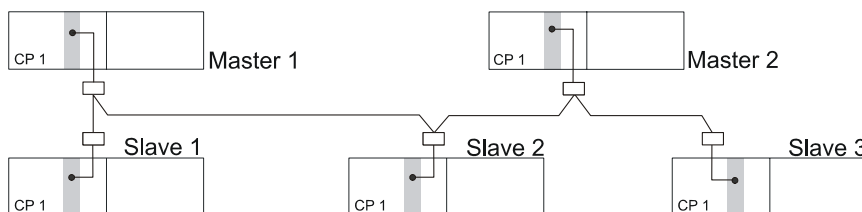
- Technically Ethernet is a point to point protocol, but by regarding hubs and switches as “part of the cable” Ethernet can be considered a multidrop link.

A multidrop link is a physical link (“cable”) that connects three or more systems.

Multidrop links open the possibility to configure multiple logical point to point links between master(s) and slave(s) connected via one multidrop link.

Figure 54 on page 289 shows an examples of a multidrop configuration with two masters and three slave systems.

Figure 54 Example of a multidrop link



Communication redundancy based on the fail-over principle

Communication redundancy fail-over is used by almost every redundant communication protocol, except SafeNet. (For SafeNet details see “Communication redundancy and SafeNet” on page 290.)

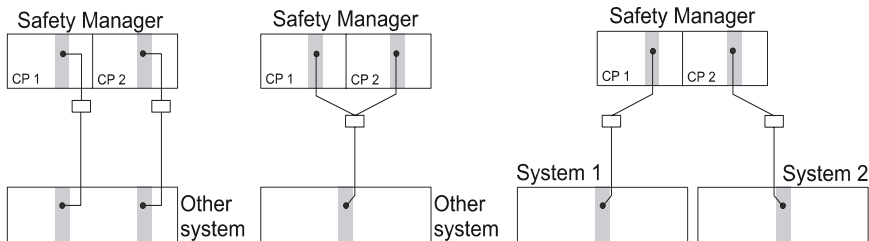
Communication redundancy fail-over is the automated capability of a device to switch over to a redundant or dormant communication path upon the failure or abnormal termination of the active path.

To determine which line is dormant and which is active a token is used by either the responder or the initiator of the communication, i.e. Safety Manager or the other system.

- When you choose **Safety Manager as the device controlling the fail-over**, you must **uncheck** the checkbox in the properties window of the device Safety Manager is connected to.
Safety Manager will swap paths roughly every ten seconds as long as the dormant path remains healthy.
If a path is diagnosed faulty, Safety Manager swaps to the remaining healthy path. A diagnostic message logs the communication failure. At the same time Safety Manager keeps trying the faulty path: As soon as the faulty path is found healthy again Safety Manager initiates a fail-back which results in both paths being used again.
- When you choose **the other system as the device controlling the fail-over**, you must **check** the checkbox in the properties window of the device Safety Manager is connected to.
Safety Manager will wait for the device to switch paths in case a communication failure takes place.

Figure 55 on page 290 shows the redundancy architectures supported by Safety Manager when applying the communication fail-over principle.

Figure 55 Supported types of redundancy



- Figure 55 on page 290 left shows a **fully redundant link**: Depending on the configuration of the other system you enable or disable *Communication redundancy fail-over* on the other system.
- Figure 55 on page 290 center shows a **shared CP link**: Since the other device has no redundant link, you disable *Communication redundancy fail-over* on the other system, unless Ethernet is used and the other system is capable of rerouting the communication to another port / IP address.
- Figure 55 on page 290 right shows a (not often used) **redundant devices link**: Here the actual data transmitted/received depends on the devices that request or send data. Since neither path is dormant, you should enable the *Communication redundancy fail-over* on “the other system”.

**Caution:**

When connecting independent devices to a redundant link as shown on the right side of Figure 55 on page 290 you should realize that:

1. Point data sent to System 1 may differ from that sent to System 2, due to the dynamic character of point data and the moment in time when requesting/processing this data.
2. When both systems write data to Safety Manager in the same application cycle the values received by CP2 prevails.
3. Connecting independent devices to a redundant link cannot be applied to SafeNet configurations.

Communication redundancy and SafeNet

**Note:**

Non-redundant SM Controllers do not support redundant SafeNet.

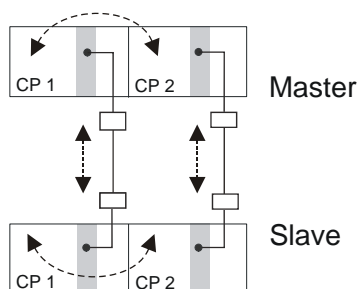
Redundant SafeNet links must be used for redundant SM Controllers.

Figure 56 on page 291 shows that data communicated via redundant SafeNet links is also shared between Control Processors, causing a redundant data flow:

- If both links are operational, the Master-Slave data flow passes via both links simultaneously. The Control Processors continuously compare and synchronize the data flows on both paths.
- If one link fails, a diagnostic message is generated and the data flow continues via the remaining healthy SafeNet link. The Control Processor with the faulty link now relies on the Control Processor with the healthy link to send/receive the data.

This results in a single-fault-tolerant communication network.

Figure 56 Data flow between SafeNet and redundant Control Processors



Communication overview

Table 11 on page 291 shows a complete overview of communication options.

Table 11 Overview of peer-to-peer connections

| Connection | Protocol | Physical network | Safe? | Data | Remarks |
|---------------------------------|----------|---|-------|--|---|
| Safety Manager - Safety Manager | SafeNet | <ul style="list-style-type: none"> • RS232 • RS485 • RS422 • Ethernet | yes | <ul style="list-style-type: none"> • safe points • non-safe points • time sync • remote load • remote reset | Logical links may span up to 7 physical links |

Table 11 Overview of peer-to-peer connections (*continued*)

| Connection | Protocol | Physical network | Safe? | Data | Remarks |
|--|----------------|---|-------|---|--|
| Safety Manager - Safety Station (Safety Builder) | Safety Builder | <ul style="list-style-type: none"> • RS232 • RS485 • RS422 • Ethernet | no | <ul style="list-style-type: none"> • data viewing • time set • diagnostics • forcing • loading | Logical links may span up to 7 physical links |
| Safety Manager - Experion TM | Experion | <ul style="list-style-type: none"> • Ethernet | no | <ul style="list-style-type: none"> • non-safe points • time sync • data viewing • diagnostics • Sequence Of Events (SOE) recording | |
| Safety Manager - CEE controller | PCDI | <ul style="list-style-type: none"> • Ethernet | no | <ul style="list-style-type: none"> • non-safe points | For peer-to-peer communication via FTE with CEE controller |
| Safety Manager - MODBUS device | MODBUS RTU | <ul style="list-style-type: none"> • RS232 • RS485 • RS422 | no | <ul style="list-style-type: none"> • non-safe points • time set | Supports both 2-wire and 4-wire RS232 links |
| | MODBUS TCP | <ul style="list-style-type: none"> • Ethernet | no | <ul style="list-style-type: none"> • non-safe points • time set | |
| Safety Manager - plant clock | PTP and NTP | <ul style="list-style-type: none"> • Ethernet | no | <ul style="list-style-type: none"> • time sync | Set the correct time zone in Plant properties |

Ethernet versus serial communication

The choice between Ethernet and serial communication is basic:

- Serial communication is often already cabled on existing sites and is thus a logical choice within the limits of existing infrastructures.
- Ethernet communication however is faster, more flexible, universal and more up to date; when restructuring your communication infrastructure or setting up a project from scratch, Ethernet is the better choice.

Ethernet communication has several advantages over serial communication. Some of these are:

- Ethernet communication allows simultaneous communication of multiple connections and protocols via one physical port. With Ethernet it is e.g.

possible to configure multiple Experion, NTP clock synchronization and Modbus TCP connections on one USI channel.

- Ethernet communication also allows multiple masters per device type (e.g. multiple Modbus masters), to address one slave.
- The communication capacity and number of connectable nodes is much higher than those for serial communication.



Note:

It is advised to keep data processing networks such as FTE, SafeNet and public (office) networks separate.

The following disadvantages of Ethernet can easily be circumvented by keeping data processing networks such as FTE, SafeNet and public (office) networks separate:

- Ethernet networks are vulnerable to intrusion due to its open standard and easy connectivity
- Public Ethernet networks can easily be overloaded causing retries, loss of data packets and delays.

Network components

Network components are elements used in Network Configurator to build the network with. Network components define:

- the network properties of the system linked to the network (For details see “Configuring Physical View component properties” on page 72 and “Configuring Logical View component properties” on page 92.)
- the function of the system as an element in the network

Covering long distances

To cover long distances, e.g. for pipe-line or off-shore monitoring, a number of technologies have been successfully applied in previous projects, such as:

- Telephone (copper) line
- Satellite uplink
- Fiber optic link

For options as how to best apply these technologies, contact Honeywell SMS.

Communication capacity

The communication to Safety Manager points is established via communication markers (DI, DO) and/or communication registers (BI, BO).

- The values of these points are stored in dedicated memory banks containing markers and registers.
- The data transfer of these marker and register values to external devices is handled by one or more SM Communication modules.

The overall communication capacity of a Safety Manager is thus determined by the available free memory and the data transfer capacity.

Communication memory

Figure 57 on page 294 shows an example screen where you allocate communication memory to a communication channel. The numbers displayed indicate the amount of memory allocated in *bytes*.

You can allocate memory in multitudes of 4 bytes.

Figure 57 Communication memory allocation per channel

The screenshot shows the 'Logical Network Properties' dialog box. It contains the following fields and sections:

- Master Node:** A dropdown menu.
- Slave Node:** A dropdown menu.
- Protocol:** A dropdown menu.
- Route:** A dropdown menu.
- Device Address:** A text field with a double dash (..) as a placeholder.
- Markers Section:**
 - In size (bytes):** A numeric spinner set to 0.
 - Out size (bytes):** A numeric spinner set to 0.
 - PLC base in:** A numeric spinner set to 0.
 - PLC base out:** A numeric spinner set to 0.
- Registers Section:**
 - In size (bytes):** A numeric spinner set to 0.
 - Out size (bytes):** A numeric spinner set to 0.
 - PLC base in:** A numeric spinner set to 0.
 - PLC base out:** A numeric spinner set to 0.
- Enable Timeout:** An unchecked checkbox.
- Timeout (ms):** A numeric spinner set to 0.
- Network delay (ms):** A numeric spinner set to 0.
- Buttons:** OK, Cancel, and Help buttons at the bottom.

The memory areas used to store communication marker and register values belong to larger memory banks, dedicated to storing *all* marker and register values.

The total amount of memory available per SM Controller for storing and communicating marker and register bytes is limited by the following factors:

1. The remaining free memory in the related marker or register memory bank (depends also on already allocated points, markers and registers on FLDs);
2. The maximum size for allocating communication memory.

The maximum size of communication memory depends on the communication type and point data:

1. For SafeNet the communication configuration per SM Controller is limited to
 - a. a maximum of 2000 bytes *Out size* for markers and registers;
 - b. 4000 bytes *In size* for markers and registers (including all logical links handled by that SM Controller).
2. For all non-SafeNet communication the communication configuration per SM Controller is limited to
 - a. a total of 508 bytes for all communication involving markers;
 - b. a total of 8188 bytes for all communication involving registers.

Allocating buffers for markers and registers

If you want two logically connected systems to exchange point data you must allocate bytes in the marker and register in and out buffers for storage of this data.




Note:

You do not need to reserve bytes for commands and messages such as load, reset, SOE, diagnostic and time synchronization related messages.

You reserve these bytes in the Logical Network Properties window.

- Always allocate spare buffer space for future expansions; once systems are on-line you cannot change the buffer size without shutting down the communication.
- “Logical View property fields explained” on page 116 has entries that provide examples to calculate marker and register buffer sizes.
- “Communication memory” on page 294 indicates the maximum size allowed per SM Controller / communication module.

Data transfer capacity for non-SafeNet related communication



Attention:

USIs running 3rd party protocols may be vulnerable to communication overflow, causing USI outages and communication shutdown.

If communication overflow is a potential risk, we recommend to allocate all SafeNet links on dedicated USIs (not running vulnerable 3rd party protocols).

The maximum amount of data that can be read from Safety Manager is limited by the capacity provided by the available protocol, the communication buffer size and communication speed.

The amount of data that a device can *write* to Safety Manager for non-SafeNet related communication, is limited by two factors:

Per second

The number of writes per second combined with the amount of data written per second. When presented as a formula you get:

$$\left(\frac{\# \text{ Writes per second}}{2} + \frac{\# \text{ Bytes written per second}}{250} \right) \leq 25$$

Per cycle

When writing non-SafeNet related communication to Safety Manager you are also limited to the following volumes *per cycle*

- writing 2792 coils/markers per cycle via marker blocks (*Mblock*) or
- writing 604 register bytes per cycle via register blocks (*Rblock*) or
- writing/forcing 64 individual points per cycle with individual commands or
- a combination of above.

When presented as a formula you get:

$$Mblock = 12 + \left\lceil \frac{Coils}{8} \right\rceil$$

The maximum number of coils per message is limited to 2040 per cycle

$$Rblock = 12 \times registerbytes$$

The maximum number of register bytes is limited to 255 per cycle

Single: A single force or write command

Mblock: Marker or coil block size (in bytes)

Rblock: Register block size (in bytes)

$$\sum_{0}^n R_{\text{block}} + \sum_{0}^m M_{\text{block}} + (10 \times \text{Single}) \leq 640_{\text{bytes}}$$

Besides the buffer size limitation, there is no limitation on the number of allocated points that can be read by an external device.

External communication failure

Logical connections to external devices are expected to be communicating continuously.

The correct operation of all logical connections is monitored by Safety Manager via time-outs, which can be defined by the user when configuring the logical connection.

A logical connection is regarded faulty if at least *one* of the Control Processors loses its connection to the device for a period longer than the configured time-out.

(This does not mean that all communication is lost; the other [redundant] Control Processor may still be able to uphold its connection and relay the correct application values.)



Note:

When troubleshooting you can access **Controller Management>Communication Status>Link Status** to see which logical connection caused the communication failure.

If (one of the lines of) a logical connection is regarded faulty:

- The fault is reported via the extended diagnostics – including a list of the logical connections lost on that channel.
- The ExtComFaultCC# alarm marker (# stands for the channel number) goes low upon first detection of a communication loss via channel #.
 - The ExtComFaultCC# alarm marker “dips” upon loss of another logical connection on that same channel. (For more information see “Alarm marker state” on page 386.)

Safety Manager automatically recovers from the external communication fault as soon as the connection is restored, unless:

- all communication to the external device was lost (including redundancy) *and* Safe communication inputs are allocated on that connection. (See “Fault

reaction and fault recovery for communication inputs” on page 298 for details).

- the connection is a SafeNet link. (See “Fault Handling” on page 327 for details.)

The diagnostic message remains in the actual diagnostics database until reset. For more information see “Diagnostic messages and databases” on page 247.

Fault reaction and fault recovery for communication inputs

If all logical connections to an external device time out, (see “External communication failure” on page 297 for details) the SM Controller no longer receives updates for its communication inputs.

From that moment on the SM Controller assumes the predefined fault reaction state on all communication inputs that depend on that logical connection.

- Other communication inputs remain unaffected.
- For an overview of fault reaction states see “Fault reaction” on page 399.



Note:

To restore a broken *SafeNet* connection you always need to reset the SM Controller, regardless the fault reaction setting of the communication inputs.

See “Fault Handling” on page 327 for details.

The response of the SM Controller when communication is (partly) restored, depends mainly on the fault reaction setting (see Table 33 on page 399):

- If one communication input has a Safe fault reaction setting of either Low, High or Fixed Value you must reset the SM Controller to restart communication.
- If all communication inputs have the Non-Safe Freeze as their fault reaction state, communication restores automatically. A reset would only be required to clear the fault database.

Communication via the Experion protocol

The Experion™ protocol is used for non-safe data communication on controller level.

Function

The Experion™ protocol is used on physically connected Safety Managers to:

- Write the states of non-safe inputs with location COM.
- Monitor the states of each Safety Manager point.
- View Safety Manager diagnostics and system parameters on an Experion Station.
- collect SOE data.
For more information see “Sequence of events (SOE)” on page 441.
- synchronize the Safety Manager real-time clock.
See “Real-time clock synchronization” on page 332 for details.

Experion



Note:

For details on Experion communication and Experion FTE, see the *Experion Safety Manager Integration Guide* in the Experion Knowledge Builder.

The Experion™ protocol is based on the PlantScape protocol that runs on Ethernet. It is primary used for communication between Experion servers and clients, such as stations, CEE controllers and Safety Manager.

Communication



Note:

1. The Experion protocol runs on top of an Ethernet TCP/IP layer.
 2. With the Experion protocol you can only communicate to physically directly connected Safety Managers.
-

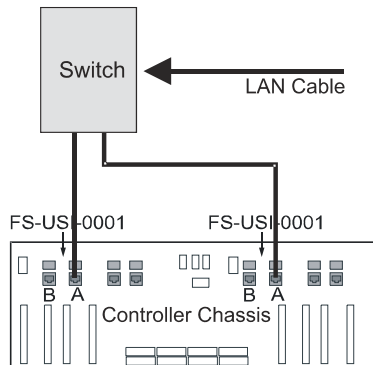
The Experion™ protocol can be run:

- on a non-redundant Ethernet network or
- on a redundant Ethernet, such as Experion FTE (Fault Tolerant Ethernet)

Architecture of a non-redundant Ethernet network

Figure 58 on page 300 shows the basic architecture of the communication link between Safety Manager and a non-redundant Ethernet network.

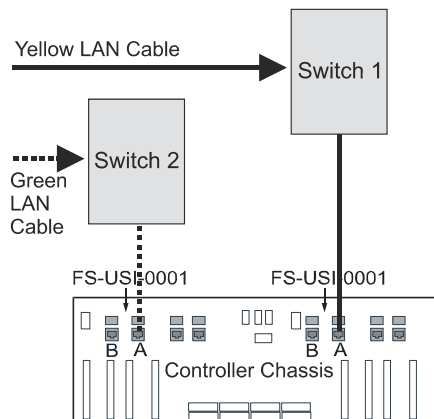
Figure 58 Connecting the Ethernet switch to the USI-0001 communication modules and the LAN



Architecture of a redundant Ethernet network

Figure 59 on page 300 shows the basic architecture of the communication link between Safety Managers and e.g. the Experion FTE network.

Figure 59 Connecting the Ethernet switch to the USI-0001 communication modules and the LAN



Data Exchange

During the communication process, Safety Manager performs a slave function, which means that data exchange is initiated by the external device, e.g. an Experion[™] server.

The data exchange between Safety Manager and Experion is realized via predefined marker and register areas (see Figure 60 on page 301). The communication link to Safety Manager application is made through application points (DI, DO, BI, or BO) with a DCS address assigned. These are allocated to the Safety Manager communication link with Experion.

Safety Manager is able to handle a maximum of 640 data bytes per read/write transfer, i.e. a maximum number of 2000 coils or 125 holding registers.

For information about Safety Manager loading capacity for i.e Modbus see “Communication capacity” on page 294.

Figure 60 Experion data area configuration

The screenshot shows the 'Logical Network Properties' dialog box with the following settings:

- Master Node:** Experion Server
- Slave Node:** SM Controller
- Protocol:** Experion
- Route:** Experion Server . PhysicalNetwork . SM Contr
- Device Address:** --
- Markers:**
 - In size (bytes): 0
 - Out size (bytes): 0
 - PLC base in: 0
 - PLC base out: 0
- Registers:**
 - In size (bytes): 0
 - Out size (bytes): 0
 - PLC base in: 0
 - PLC base out: 0
- ☒ **Enable Timeout**
 - Timeout (ms): 1000
 - Network delay (ms): 0

Buttons at the bottom: OK, Cancel, Help.

Allocating

For details on how to allocate an SM Controller or Safety Manager points on Experion™, refer to the Experion documentation.

SM Controller allocation

To allocate an SM Controller you must create coil and register controllers in Experion that relate to Safety Manager.

If SOE is enabled you must also create a SOE controller in Experion.

Point allocation

To allocate IO points you must copy the point PLC addresses, that you assigned via Point Configurator, in the related coil, register and SOE controllers that you created in “SM Controller allocation” on page 302.

- Points of type DI and DO can be assigned in the range of 1 to 8192.
- Points of type AI, BI, BO and AO can be assigned in the range of 10001 to 18192.

Fault handling

Communication channels that are configured for the Experion™ protocol are expected to be communicating continuously. When time-outs are enabled, the correct operation of these communication channels is monitored by Safety Manager.

Figure 60 on page 301 shows the location of the time-out setting. Time-outs can be enabled by checking the *Enable timeout* check box and setting a time-out value in the communication channel properties between 500 ms and 30.000 ms (half a minute).

A channel is regarded faulty if no valid frame was received within the configured time-out period.

- The fault reaction state will be assigned to all inputs from Experion.
- The fault is reported via the extended diagnostics and the DEVICE-COM.FLT alarm marker.

The system automatically recovers from this fault as soon as communication is re-established. The diagnostic message remains.

Communication via the Peer Control Data Interface

The Peer Control Data Interface (PCDI) is a Honeywell licensed communication interface for non-safe peer to peer data communication between Experion CEE controllers and SM Controllers.

The C300 is an Experion CEE controller that can be equipped with a licensed PCDI. With PCDI, the C300 can:

- write the states of non-safe inputs with location COM,
- monitor the states of each Safety Manager point that has been assigned a COM output to the CEE controller,
- monitor Safety Manager system parameters that have been assigned a PLC address to the CEE controller.

PCDI



Note:

A separate license is required for PCDI support in Experion. Such a license is not required for Safety Manager.

Information exchange with PCDI is done with blocks. Each block contains the following information:

- System address
- Command type (function code)
- Function parameters
- Checksum

The length of a block depends on the function code and the function parameters. The checksum is used to verify the correctness of the transferred information.

For more information on PCDI see the Experion Knowledge Builder:

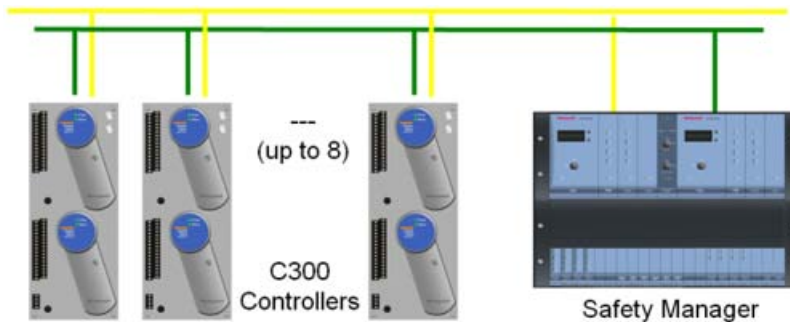
- The *Experion Safety Manager Integration Guide* for an overview of instructions for setting up a PCDI link with a CEE controller,
- The *Peer Control Data Interface Implementation Guide* for general information about PCDI.

Communication architecture

Figure 61 on page 304 shows how PCDI is supported on redundant Ethernet networks such as FTE.

You can configure up to 8 PCDI masters per physical (USI) Ethernet channel.

Figure 61 Safety Manager–CEE communication via a redundant FTE network



Data exchange

During the communication process Safety Manager performs a slave function, which means that data exchange is initiated by the CEE controller(s).

- Safety Manager supports up to eight CEE controllers per channel.

For information about Safety Manager loading capacity for PCDI see “Communication capacity” on page 294.

Supported function and error codes

Table 12 on page 304 and Table 13 on page 305 list the PCDI function and error codes supported by Safety Manager.

Table 12 Supported PCDI function codes

| Code | Description |
|-------|-----------------------|
| 1 | read coil status |
| 2 * | read input status |
| 3 ** | read holding register |
| 4 *** | read input register |
| 5 | force coil |
| 6 | load register |
| 8 | loop back test |

Table 12 Supported PCDI function codes (*continued*)

| Code | Description |
|------|--------------------------|
| 15 | force multiple coils |
| 16 | force multiple registers |

- * Function code 2 is handled the same way as function code 1.
- ** If no register with the defined PLC address exists a coil PLC address is used instead, causing a coil to be read instead of a register.
- *** Function code 4 is handled the same way as function code 3.

Table 13 Supported PCDI error codes

| Code | Description | Cause |
|------|-----------------------|--|
| 1 | Illegal function code | An unsupported function code is applied. |
| 2 | Illegal data address | The applied variable address exceeds the configured communication area boundaries. |
| 3 | Illegal data value | Incorrect data format (e.g. Not a Number (NaN) and Infinite (Inf)). |
| 6 | Busy | Data cannot be accepted at this time. |

Response to illegal values

When Safety Manager receives an illegal value

- the communication block containing that value is discarded and
- a Code 3 (Illegal data value, see Table 13 on page 305) is sent in return.

Examples of illegal values are: Not a Number (NaN) and Infinite (Inf).

Writing to communication inputs



Attention:

To re-establish a broken communication link you need to reset the SM Controller if communication inputs are configured with a fault reaction setting other than **Freeze**.

- If all communication inputs are configured with fault reaction setting **Freeze** communication will be re-established automatically.

In Safety Manager you must assign a fault response to each communication input point.

When the communication link to a CEE controller times-out, Safety Manager will assign the fault response value to the communication input. As soon as communication is re-established, the CEE controller should correct that value.

Table 14 on page 306 shows the possible fault reaction settings for communication IO.

Table 14 Fault Reaction settings for communication IO

| Signal type | Fault Reaction settings |
|---|-------------------------|
| Digital Points (DI) | High/Low/Freeze |
| Numeric Points (BI) (The default fixed value for numerics is 0.) | Fixed Value/Freeze |



Attention:

A C300 Controller writing to a communication input of Safety Manager, may not be configured with the C300 setting `WriteOnChange` active.

- Use `WriteAlways` or `WriteOnDiff` instead.

For more information see the *Peer Control Data Interface Implementation Guide* in Experion Knowledge Builder.

With `WriteOnChange` the C300 controller does not look at the current value used by Safety Manager (which might have changed due to a fault reaction value after a detected time-out).

Honeywell SMS recommends to use the setting `WriteAlways` or `WriteOnDiff` instead:

- `WriteOnDiff` is preferred as this reduces the required write actions to Safety Manager to a minimum. (See “Data transfer capacity for non-SafeNet related communication” on page 296 for more information.)

Configuring addresses and response times

Part of setting up the logical connection configuration is configuring the addressing and response time schemes as shown in Figure 62 on page 307:

- Device address
- PLC addresses
- Timeout
- Network delay

Figure 62 PCDI addressing and time-out schemes

Logical Network Properties

Master Node: CEE Controller

Slave Node: SM Controller

Protocol: Peer Control Data Interface

Route: CEE Controller . PhysicalNetwork . SM Contro

Device Address: 2

Markers

In size (bytes): 0

Out size (bytes): 0

PLC base in: 0

PLC base out: 0

Registers

In size (bytes): 0

Out size (bytes): 0

PLC base in: 0

PLC base out: 0

☒ Enable Timeout

Timeout (ms): 1000

Network delay (ms): 0

OK Cancel Help

Device address

Within the logical configuration, the address of the target Safety Manager that the CEE controller wants to communicate with must be specified.

The communication address of Safety Manager is defined in the **Device Address** field in the **Logical Network Properties** window, as shown in Figure 62 on page 307.

PLC addresses

- The CEE controller marker PLC addresses range from 1 to 65535.
- The CEE controller register PLC addresses range from 1 to 65535.
Long Words and Floats get 2 PLC addresses assigned. The most significant value in the sequence is stored at the lowest storage address.

For information as how to set these addresses see “Communication allocation” on page 403.

Timeout



Tip:

Rule of thumb is to take the configured time-out in the CEE controller, multiply this value by 2 and add one second.

The resulting value is the time-out to be filled in the SM Controller **Timeout (ms)** box.

The response time has to be set in the **Timeout (ms)** box of the **Network Logical Properties** window.

Typical values are between 3 – 60 sec.

Network delay

Network delay indicates the known lag in communication.

For more information see “Network delay (ms)” on page 122.

Fault handling

For details on fault handling see

- “External communication failure” on page 297
- “Fault reaction and fault recovery for communication inputs” on page 298

Communication via the Modbus protocol

The Modbus protocol is used for non-safe data communication to 3rd party equipment such as PLC's, SCADA and (non Honeywell) DCS systems.

The Modbus protocol can be used by external systems to:

- Write the states of non-safe inputs with location COM.
- Monitor the states of each Safety Manager point that has been assigned a COM output to the Modbus device
- Monitor Safety Manager system parameters that have been assigned a PLC address to the Modbus device
- Set the real time clock of the SM Controller.
See “Real-time clock synchronization” on page 332 for details.

Modbus TCP and Modbus RTU



Note:

Modbus RTU auto detects and supports both 2-wire and 4-wire RS232 configurations.

Safety Manager supports the following Modbus protocols:

- Modbus TCP; runs on Ethernet based networks.
- Modbus RTU; runs on serial networks, such as RS232, RS422 and RS485.

The Modbus protocol as implemented in Safety Manager conforms to the description in the Gould Modbus protocol reference guide.

Communication architecture



Note:

Multidrop is only supported via Ethernet and RS485

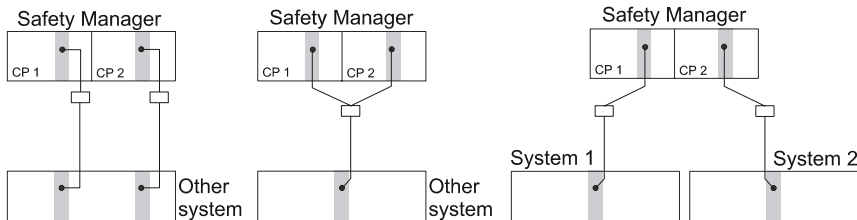
Modbus can be run on Ethernet, RS232, RS422 and RS485.

- When run on Ethernet you can configure up to 8 Modbus masters per physical (USI) Ethernet channel.

The Modbus communication protocol is supported on both point-to-point and multidrop networks and can be configured redundant or non-redundant.

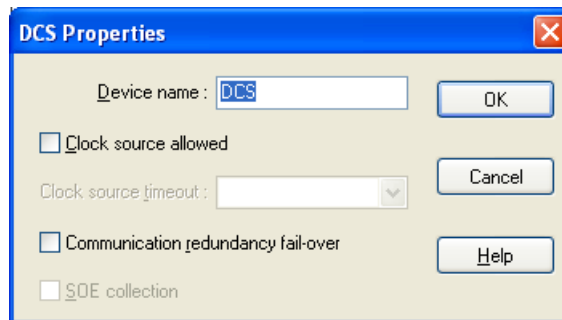
Figure 63 on page 310 shows the supported redundant communication configurations. For details on configuring these configurations see “Communication redundancy based on the fail-over principle” on page 289.

Figure 63 Connection examples with a redundant Safety Manager



- When configuring a form of redundant communication you must set the *Communication redundancy fail-over* box in Figure 64 on page 310 as described in “Communication redundancy based on the fail-over principle” on page 289.
- When building a non-redundant communication link you must **uncheck** the *Communication redundancy fail-over* box in Figure 64 on page 310.

Figure 64 the Modbus Communication redundancy fail-over box



Data exchange



Note

When Safety Manager receives an unsupported value the communication block containing that value is discarded and a Code 3 (Illegal date value, see Table 16 on page 312) is sent in return.

Examples of unsupported values are: Not a Number (NaN) and Infinite.

During the communication process Safety Manager performs a slave function, which means that data exchange is initiated by the Modbus device.

- Safety Manager supports up to eight Modbus TCP controllers per channel.
For information about Safety Manager loading capacity for Modbus TCP see “Communication capacity” on page 294.

Use of frames

Information exchange within the Modbus protocol is accomplished in frames. Each frame contains the following information:

- system address,
- command type (function code),
- function parameters, and
- checksum (CRC-16).

The length of a frame depends on the function code and the function parameters. The checksum is used to verify the correctness of the transferred information.

Function and error codes used to support data exchange

Table 15 on page 311 and Table 16 on page 312 lists the Modbus function and error codes supported by Safety Manager.

Table 15 Supported Modbus function codes

| Code | Description |
|-------|--------------------------|
| 1 | read coil status |
| 2 * | read input status |
| 3 ** | read holding register |
| 4 *** | read input register |
| 5 | force coil |
| 6 | load register |
| 8 | loop back test |
| 15 | force multiple coils |
| 16 | force multiple registers |

* Function code 2 is handled the same way as function code 1.

** If no register with the defined PLC address exists a coil PLC address is used instead, causing a coil to be read instead of a register.

*** Function code 4 is handled the same way as function code 3.

Table 16 Supported Modbus error codes

| Code | Description | Cause |
|------|-----------------------|--|
| 1 | Illegal function code | An unsupported function code is applied. |
| 2 | Illegal data address | The applied variable address exceeds the configured communication area boundaries. |
| 3 | Illegal data value | Incorrect data format (e.g. invalid time stamp). |
| 6 | Busy | Data cannot be accepted at this time. |

For a detailed description of the supported function codes (including function parameters and frame formats) refer to the Modbus Gould protocol reference guide.

Configuring addresses and response times

Part of setting up the logical connection configuration is configuring the addressing and response time schemes as shown in

- Device Address
- PLC Addresses

Another option of Safety Manager is the support of packaged coils as described in “Packaged Coils” on page 314.

Figure 65 Configuring Modbus addressing and time-out

Logical Network Properties

Master Node: DCS

Slave Node: SM Controller

Protocol: Modbus

Route: DCS . PhysicalNetwork . SM Controller

Device Address: 3

| Markers | | Registers | |
|-------------------|---|-------------------|---|
| In size (bytes): | 0 | In size (bytes): | 0 |
| Out size (bytes): | 0 | Out size (bytes): | 0 |
| PLC base in: | 0 | PLC base in: | 0 |
| PLC base out: | 0 | PLC base out: | 0 |

☒ Enable Timeout

Timeout (ms): 1000 Network delay (ms): 0

OK Cancel Help

Device Address

Within the logical configuration, the address of the target Safety Manager that the Modbus master wants to communicate with must be specified.

The communication address of Safety Manager is defined in the **Device Address** field in the **Logical Network Properties** window, as shown in Figure 65 on page 313.

PLC Addresses


The address ranges for coils and registers comply to the Modbus Gould specification.

- The Modbus marker PLC addresses range from 1 to 65535.
- The Modbus register PLC addresses range from 1 to 65535. Long Words and Floats get 2 PLC addresses assigned. The most significant value in the sequence is stored at the lowest storage address.

- The address ranges 9996 – 9999 and 49996 – 49999 are reserved for clock synchronization.

Packaged Coils

Safety Manager supports the option of packaged coils. This means that multiple coils can be packed and accessed with a single Modbus function code, saving allocation space in Modbus masters that support packaged coils.



Note:

When coil and register address ranges as described in “PLC Addresses” on page 313 overlap you *cannot* use the packaged coils feature.

If you do, the register is addressed instead.

To make use of packaged coils address the first (LSB) coil using a register function code. The function code is applied to (a number of) the 16 coils addressed by the register.

Example

Modbus command 04 04 0001 0003 reads the first 3 *registers* as of PLC address 0001

As PLC address 0001 is not allocated as a register address, Safety Manager prompts the values of coils on PLC addresses 0001 through 0048 (equivalent of 3x 16 bit registers).

Below table shows the allocation of each coil when sending 48 coils packaged in 3 registers.

| Packaged Coil | address | MSB register byte | | | | | | | | LSB register byte | | | | | | | |
|---------------|---------|-------------------|----|----|----|----|----|----|----|-------------------|----|----|----|----|----|----|----|
| Register 1 | 0001 | 08 | 07 | 06 | 05 | 04 | 03 | 02 | 01 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 09 |
| Register 2 | 0017 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 |
| Register 3 | 0033 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 |

Timeout

The response time has to be set in the **Timeout (ms)** box of the **Network Logical Properties** window.

**Tip:**

A rough indicator is to determine the standard delay time between two communication sessions, initiated by the Modbus master and responded to by SM Controller, and then multiply this time by 2.

The resulting value is the time-out to be filled in the **Timeout (ms)** box.

Typical values are between 1 – 60 sec.

Network delay

Network delay indicates the known lag in communication.

For more information see “Network delay (ms)” on page 122.

Real-Time Clock Time Set**Attention:**

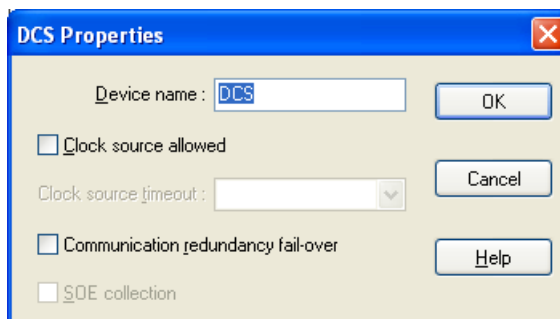
The accuracy of the real-time clock (RTC) of Safety Manager is 1ms.

The synchronization accuracy between the Modbus device and Safety Manager is *1 second + network delay*. Network delays are not compensated.

For more information see “Real-time clock synchronization” on page 332 for details.

Time set signals can be accepted from the Modbus device if the Clock source allowed box is checked. The actual update frequency depends on the type and settings made in the connected Modbus device.

Figure 66 the Modbus Communication redundancy fail-over box



The real-time clock of Safety Manager can be set by the DCS system via the Modbus register write function codes 6 or 16 with specific register addressing as defined in Table 17 on page 316.



Tip:

It is possible to allocate (word) registers (BI-COM) on addresses 9996 – 9999 and use these registers for clock synchronization simultaneously.

The advantage would be that these registers then always hold the last time set value, and this can be read-back either via Modbus or the application logic.

Table 17 Content of real time clock reserved registers

| Register address | type | content |
|------------------|-------------|---|
| (4)9996 | Year | Decimal value, e.g. 2007 |
| (4)9997 | Month/Day | Decimal value, e.g. 0812 means August 12 |
| (4)9998 | Hour/Minute | Decimal value, e.g. 2233 means 22.33h or 10.33 PM (a 24-hour clock setting is used) |
| (4)9999 | Sec./00 | Decimal value, e.g. 5900 means 59 sec. |

For more details on real-time clock synchronization refer to “Real-time clock synchronization” on page 332.

For a description of function code 6 and function code 16 interpretation see:

- Using function code 6 to set the real time clock
- Using function code 16 to set the real time clock

Using function code 6 to set the real time clock

If you use function code 6 to set the real time clock you set the first 3 registers with the content as defined in Table 17 on page 316.

Only after receipt of the last register (Sec. /00) Safety Manager validates the time stamp and synchronizes to this new date and time.

Using function code 16 to set the real time clock

If you use function code 16 to set the real time clock you set all 4 registers with the content as defined in Table 17 on page 316.

Safety Manager will synchronize immediately after receipt and validation of this new date and time.

Fault Handling

For details on fault handling see

- “External communication failure” on page 297
- “Fault reaction and fault recovery for communication inputs” on page 298

Link Types and Baud Rates

Table 18 on page 317 presents the various configuration options for the Modbus RTU communication protocol.

Table 18 Configuration options for the Modbus RTU protocol

| Link type | Supported baud rates |
|-----------|-------------------------------------|
| RS422/485 | 4800, 9600, 19k2, 38k4, 57k6, 115k2 |
| RS232 | 4800, 9600, 19k2, 38k4 |

Please note the following considerations:

1. The link can either be redundant or non-redundant. However, a redundant link is implicitly considered to be a multidrop link.
2. The number of stop bits (1, 2) bits per character (7, 8) and parity type (odd, even, none) are configurable.

Communication via the SafeNet protocol

Safety Managers can be connected together to form safety-related networks. The protocol used for this network is called SafeNet.

SafeNet is available to Safety Managers for:

- Distributed processing
- Sharing safe data for joint SIS related tasks.
- SIL3, TUV approved, communication.
- Remote load

The protocol includes timing restrictions and a high level of error detection and recovery, which makes it suitable for exchanging safe information while maintaining optimum availability.

The SafeNet protocol, in combination with RS232, can also be used in network configurations where large time delays are to be expected, e.g. modem communication, communication over telephone lines, satellite links, etc. For more information see “Low baud rate communication” on page 322.

The Safety Manager communication network is configured during the configuration of the application, by defining the interconnections between Safety Managers and the parameters of the SafeNet protocol.

The exchange of application information is realized via input points (DI, BI) and output points (DO, BO) as described in “Data Exchange” on page 323.

Communication



Attention:

USIs running 3rd party protocols may be vulnerable to communication overflow, causing USI outages and communication shutdown.

If communication overflow is a potential risk, we recommend to allocate all SafeNet links on dedicated USIs (not running vulnerable 3rd party protocols).

SafeNet can be run on the following physical data layers:

- Ethernet
- RS232; RS422; RS485

For more information about the different protocols see

- “Ethernet versus serial communication” on page 292

- “Protocol versus response time” on page 324
- “Link Types and Baud Rates” on page 328 and

Architecture

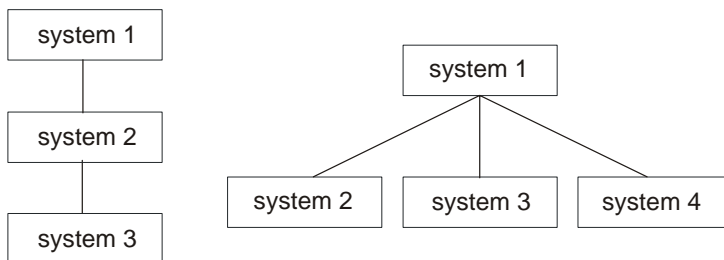


Note:

1. Multidrop is supported via RS485 and Ethernet.
2. Up to 15 slaves may be connected via a physical multidrop link based on RS485. The actual number of slaves depends on the baud rate and amount of exchanged data.

Figure 67 on page 319 shows the basic architectures available to link Safety Managers via SafeNet.

Figure 67 Examples of a point-to-point and a multidrop architecture



The following must be considered when designing SafeNet:

- You can connect Safety Managers in pairs (point-to-point), as shown left in Figure 67 on page 319 or you can connect multiple Safety Managers to the same link (multidrop), as shown right in Figure 67 on page 319.
- In a single network you can (physically and logically) connect up to 63 systems with unique system numbers.
- A logical link between master and slave can cross 4 physical layers.
- Each physical layer can have its own data layer protocol.
- If one system in an Safety Manager network has a redundant configuration, all communication links must be redundant.

Master/slave

In a SafeNet configuration, every communication link has one Safety Manager operating as a master and the other system(s) operating as slaves. The master sends data to a slave and initiates a request for data from that slave. The slave

sends data after receipt of the data request from the master. Data integrity is ensured by the SafeNet protocol.

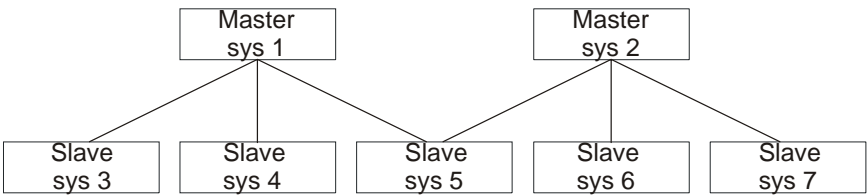
Figure 68 on page 320 shows that:

- Several slaves may be connected to one master.
- One slave may have multiple (logical) masters

The maximum number of Safety Managers (master + slaves) in a network is 63.

All Safety Managers that are connected to each other must have a unique system number.

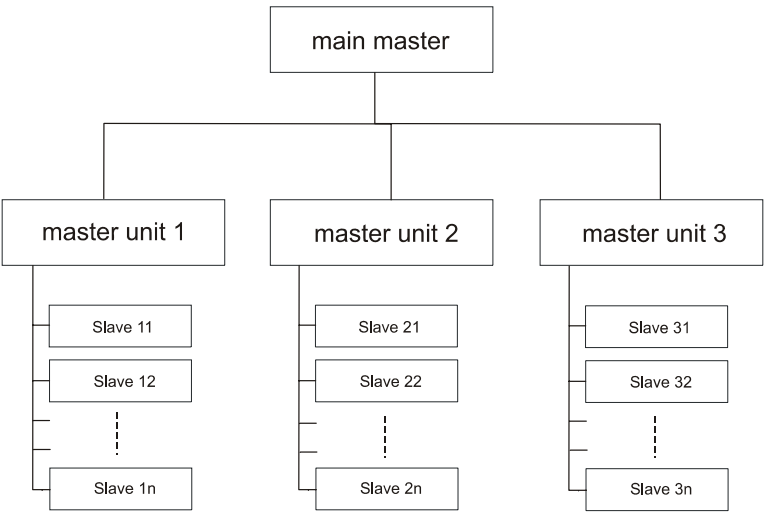
Figure 68 7 Safety Managers in a master/slave interconnection



When both redundant links are healthy, communication is established via both links alternately. If one link fails, communication is realized via the healthy link.

Figure 69 on page 320 shows an example of a typical network configuration.

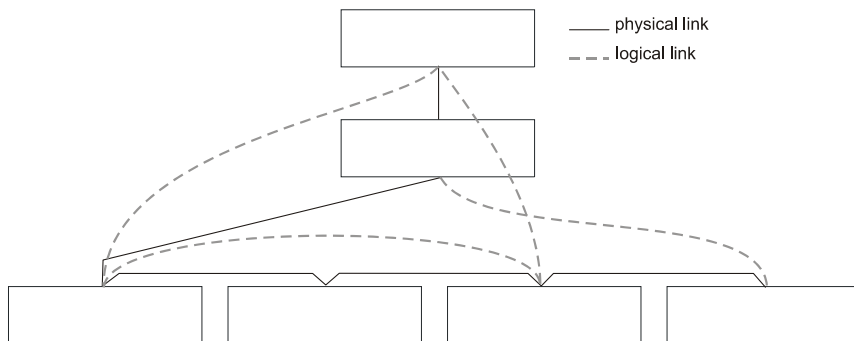
Figure 69 A typical SafeNet configuration



Physical versus s

Figure 69 on page 320 shows how Safety Manager distinguishes between physical links and logical links.

Figure 70 Physical and logical links



Physical and logical link views are equally important but differ in functionality:

- A logical link forms a virtual connection between two systems that exchange data.
 - Time-outs and response times are based on the amount of data assigned to the logical link
 - Logical links can be defined between a master and a slave, and between two SM Controllers acting as slave peers (in which case one slave becomes the master of the other)
 - A logical SafeNet link may span up to 7 physical links

The dashed connection lines in Figure 69 on page 320 provide examples of logical links.

- The physical link includes all components required to create the physical connection of systems within the network.
 - Physical links determine the transport protocol(s) used and communication speed of that (those) link(s).
 - Multiple logical links can be realized across a physical link.
 - Multiple physical links can be used to realize a logical link.

Redundant communication



Note:

Non-redundant SM Controllers do not support redundant SafeNet.

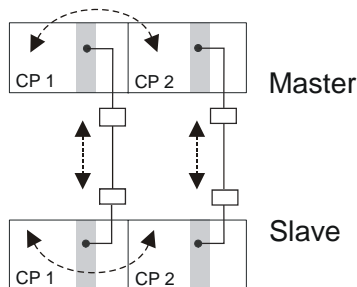
Redundant SafeNet links must be used for redundant SM Controllers.

Figure 71 on page 322 shows that data communicated via redundant SafeNet links is also shared between Control Processors, causing a redundant data flow:

- If both links are operational, the Master-Slave data flow passes via both links simultaneously. The Control Processors continuously compare and synchronize the data flows on both paths.
- If one link fails, a diagnostic message is generated and the data flow continues via the remaining healthy SafeNet link. The Control Processor with the faulty link now relies on the Control Processor with the healthy link to send/receive the data.

This results in a single-fault-tolerant communication network.

Figure 71 Data flow between SafeNet and redundant Control Processors



Low baud rate communication

Low baud rate communication is used in those applications where high baud rates are not possible. This may have a number of reasons:

- The type of cable that is used for communication is not suited for high baud rate communication.
- The communication takes place over long distances.
- There is intermediate equipment that does not support high baud rate communication.
- Multiple communication channels are sent via one communication line (using multiplexing), which means that the baud rate of the channels is smaller than that of the communication line.

Data Exchange

Figure 72 on page 323 shows that data exchange between the master and the slave is realized via predefined marker and register areas.

These areas define the pool size of marker points (DI, DO) and register points (BI and BO) with location FSC, allocated for communication with the other system.

Figure 72 Setting predefined marker and register areas for SafeNet

To exchange application information you use input (DI, BI) and output points (DO, BO) with location FSC. These input and output points are then included in the functional logic diagrams (FLDs).

The configuration of the data areas and contained points is accomplished via **Network properties** in Network Configurator.

Addressing

System addressing

A master can address one of its slaves for data-exchange.

To contact a slave for data-exchange a logical connection must exist between master and slave.

Point addressing



Note:

When allocating a point to SafeNet the tag name and allocation of that point changes in the receiving SM Controller.

In the receiving SM Controller the point gets

1. the location FSC;
2. a prefix containing the *name* of the originating SM Controller and a dot.

Example:

You want to send the value of a digital input (DI), tagged **10-HS-001** with location FLD, from the slave system, called **slave**, to the network master, called **master**.

In the slave system, called **slave**, you have therefore assigned a communication allocation on that digital input to the network master called **master**.

1. In the **slave** this point is known as **10-HS-001** with location FLD;
 2. In the **master** this point is known as **slave.10-HS-001** with location FSC.
-

The configuration of the master and slave systems must be consistent, i.e. the size of the marker/register output area in one system must be equal to the size of the marker/register input area in another system. Also, the tag numbers of the output points (DO, BO) in one system must match the tag numbers of the corresponding input points (DI, BI) in the other system.

Note that you do not apply PLC addresses to a point: This is controlled and maintained by Network Configurator automatically.

Protocol versus response time

The response time between master and logical slave depends on:

- the application program cycle time of the master and slave system in the logical link.
- the delay caused by the data layer protocol of the physical links.

Response time and time-out time are related.

The minimum time-out depends on the system application cycle and the type of communication link.

The time-out time you set must be larger than the maximum response time.

The response time to a communication request highly depends on the actual states of both master and slave system at the time of the request.

The maximum response time equals the sum of:

- the application cycle time of the master plus
- the application cycle time of the slave plus
- the expected communication delay.

The master periodically sends data to the slave systems and initiates a request for data from the slaves. An answer is expected within the time-out period; when not received in time, the link is regarded faulty.

A new data transmission and request for a slave are initiated after the slave reply to the previous request has been received. This could be equal to the time-out time, but usually it is shorter.

SafeNet time-out time

All systems within the network monitor the operation of a communication link by means of a time-out.

- The time-out can be set for each individual logical link and must be chosen such that it stays within the Process Safety Time (PST) for the Safety Instrumented System (SIS) functions involved.
- The time-out time set must be at least 2x the calculated response time.

Ethernet communication

When communicating via Ethernet you should be aware of the following:

- “Ethernet communication risks” on page 325
- “Ethernet bandwidth and response time calculation” on page 326

Ethernet communication risks



Attention:

USIs running 3rd party protocols may be vulnerable to communication overflow, causing USI outages and communication shutdown.

If communication overflow is a potential risk, we recommend to allocate all SafeNet links on dedicated USIs (not running vulnerable 3rd party protocols).

When devices communicate via an Ethernet based local area network (LAN), their information is contained and sent in packets. This is no different when using SafeNet through Ethernet. However, Ethernet has far less timing restrictions and, when sending SafeNet packets together with other application packets, some packets may suffer critical delay or get lost if a network gets congested.

Packet losses and network congestion may occur if e.g.:

- several devices start transmitting packets at the same time and/or,
- a single device generates a peak in network traffic,



Attention:

1. Risks are involved when using SafeNet on an *insecure, open or shared* Ethernet, where downtime, delays, loss and/or access to packets can be caused by other devices on the LAN.
Such risks can be caused by office computers, network printers, servers and open access points (such as wifi access points, WAN routers, etc.)
 2. Viruses and applications such as MSN Messenger may affect SafeNet reliability when active on the same Ethernet.
-

When the Ethernet is dedicated to a single Safenet, issues do not take place:

- No single SafeNet configuration can cause a 100MB Ethernet to operate at its maximum capacity (Safety Builder checks this in the configuration stage).

Packets are vulnerable to modifications or alterations when accessed by external systems: Applications running on these systems could (deliberately or via a virus infection) intercept, delay and/or alter packets.

Ethernet bandwidth and response time calculation

Please consult the release notes issued with your Safety Builder software for ways to determine bandwidth and response time.

Conventional serial communication

Please consult the release notes issued with your Safety Builder software for ways to determine bandwidth and response time.

Real-Time Clock Synchronization



Note:

The accuracy of the real-time clock (RTC) is 1ms.

The real-time clock of all Safety Managers interconnected in a SafeNet network can be synchronized. The synchronization accuracy between Safety Managers in a SafeNet network is < 10 ms.

For details on real-time clock synchronization refer to “Real-time clock synchronization” on page 332.

Fault Handling

For more information see also

- “External communication failure” on page 297
- “Fault reaction and fault recovery for communication inputs” on page 298

Fault handling



Note:

If communication fails via all links, the communication points DI and BI are set to the predefined Fault Reaction state.

Safety Manager monitors the operation of its physical communication links by means of a time-out, as discussed in “SafeNet time-out time” on page 325.

Failure of a physical link is reported via the extended diagnostics and the `ExtComFaultCC#` alarm marker, where # indicates the ID of the Control Processor involved. The report also states the system numbers of all SM Controller for which a logical connection was defined across the physical link.

Redundant links

Within redundant configurations, the communication is preserved as long as one of the links is healthy.

If communication fails on both links – i.e. communication to a connected system fails – then the value of all input points (DI, BI) that are allocated to that system are forced to their fault reaction state.

Link Types and Baud Rates

Table 19 on page 328 presents the configuration options for the SafeNet protocol.

Table 19 Configuration options for SafeNet protocol

| Link type | Supported baud rates |
|-----------|---|
| Ethernet | 100Mb full duplex |
| RS422/485 | 19k2, 38k4, 57k6, 115k2, 50k, 125k, 1M, 2M, 4M |
| RS232 | 9600, 19k2, 38k4 |

Communication via the Safety Builder protocol

The Safety Builder protocol is used for communication between Safety Station and Safety Manager.

Communication between the Safety Station and Safety Manager may be required for a number of reasons:

- monitor process behavior,
- monitor Safety Manager status,
- read/load Safety Manager diagnostics
- load an application into Safety Manager,
- force/write variables,
- set the real time clock (RTC).

Communication

The Safety Builder protocol can be run on the following physical data layers:

- Ethernet
- RS232; RS422; RS485



Note:

Multidrop is only supported via RS485 and Ethernet.

Communication between Safety Manager and the Safety Station supports both point-to-point and multidrop networks connected to one or all Control Processors of a (redundant) Safety Manager.

A Safety Station running the Safety Builder protocol can connect via:

- a physical link to Safety Manager
- a configured logical connection on SafeNet to Safety Manager

For more information on link types see “Link types” on page 287.

Data Exchange

In the communication with the Safety Station, Safety Managers perform a slave function: Data is only sent at the request of the Safety Station.



Notes:

1. If multiple links are available Safety Builder will choose the fastest operational communication link.
2. Safety Builder communication failures are reported via the Safety Station, *they are not reported by the diagnostics.*

Figure 73 Communication to a CP can be routed direct or via the other CP

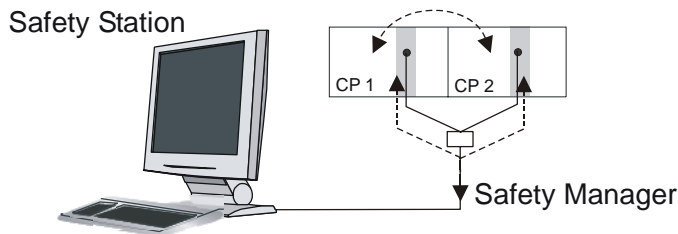


Figure 73 on page 330 shows the available communication paths:

- When addressing a specific CP (e.g. to read or load CP related data):
 - A direct link is established to that Control Processor
 - If direct communication to that CP fails, communication is realized via the redundant Control Processor.
 - If all communication fails Safety Builder will prompt an error message.
- When reading/writing process related data over a redundant link, communication will be established via both links alternately.
 - A changeover to the other link is typically attempted every 10 seconds.
 - If communication via one of the links fails, all communication is realized via the remaining healthy link.
 - If all communication fails Safety Builder will prompt an error message.

Addressing

Node addressing

The target system(s) for the Safety Station to communicate with is/are determined by the currently selected system in the Safety Builder on-line option.

The system number is used as a reference to address the target system.

The low level addressing method is determined by the data layer protocol running on the used communication link. If Ethernet communication is used, both the IP address and the system number must match.

Point addressing

- The Safety Builder marker PLC addresses range from 0 to 29999.
- The Safety Builder register PLC addresses range from 32000 to 65534.

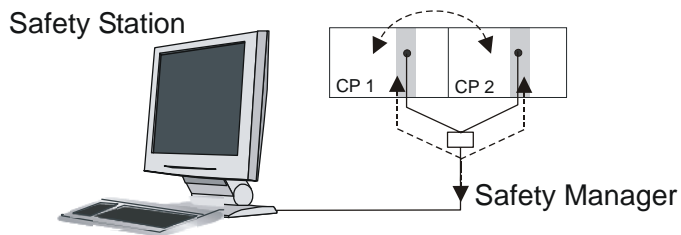
Fault Handling

If a communication channel has only been configured for communication with the Safety Station, then Safety Manager does *not* monitor the operation of the communication channel.

Safety Manager reports broken links with Safety Station, when the communication is set-up as shown in Figure 74 on page 331.

- Communication failures are not reported when Ethernet is used.

Figure 74 Communication failures are reported in this type of configuration



Link Types and Baud Rates

Table 20 on page 331 presents the configuration options for the Safety Builder protocol.

Table 20 Configuration options for Safety Builder protocol

| Link type | Supported baud rates |
|-----------|-------------------------------|
| Ethernet | 100Mb full duplex |
| RS422/485 | 9600, 19k2, 38k4, 57k6, 115k2 |
| RS232 | 9600, 19k2, 38k4 |

Real-time clock synchronization

The real-time clock of Safety Manager has a resolution of 1ms.

In order to ensure accurate time-stamping of data, the real-time clock of Safety Manager can be synchronized with a reference clock.

Safety Manager accepts several external clock sources to synchronize (set) its real-time clock to:

- an NTP/PTP based time server
- a SafeNet master
- A Modbus device
- an ExperionTM server
- A Safety Station

The following topics are discussed in this appendix.

| Topic | See |
|---|----------|
| Clock source properties | page 332 |
| PTP/NTP based time servers | page 335 |
| SafeNet | page 337 |
| Experion server | page 339 |
| Modbus | page 340 |
| Safety Station | page 341 |
| Setting time synchronization in Experion environments | page 341 |

Clock source properties

Update frequency and accuracy

The clock sources periodically give time synchronization commands to Safety Manager. The frequency and accuracy in which this is done depends on the time source used.

**Note:**

Time-out properties must be set such that they overlap the update frequency.

Table 21 on page 333 provides an overview of these properties for the various clock synchronization sources.

Table 21 Update frequency of time synchronization signals

| Source | Frequency | accuracy |
|---------------------------|---|--------------------------|
| PTP/NTP based time server | The time synchronization update frequency depends on the settings in the commercially available time server. Time synchronization happens <2 seconds. | PTP: 10ms NTP: 100ms |
| SafeNet | The time master assigned in SafeNet issues a time synchronization signal at least every 64 seconds. | 10ms |
| Experion server | Experion [™] issues a time synchronization signal to Safety Manager: 1. As soon as the communication link is (re)established (at system startup, and every time the Safety Manager enable status on the Experion display is cycled), and 2. Every 24 hours at a user-defined number of minutes after midnight. | 1 second + network delay |
| Modbus | Time synchronization is to be initiated by the Modbus device. The actual update frequency depends on the type and settings made in the connected Modbus device. | 1 second + network delay |
| Safety Station | Time synchronization signals must be given manually from a Safety Station, via the Controller Management menu. | 1 second + network delay |

Adapted time zone, daylight saving and format



Note

When applied, daylight saving correction should be enforced by sending a time synchronization signal containing the new time when the hour shifts.

- When using NTP, PTP and/or SafeNet timing protocols the time zone and date format applied depends on the settings made in Safety Manager.
- When using Experion[™] Server, Modbus or Safety Builder for time synchronization, a time synchronization signal is expected to contain the correct date and time format and represent the current local time.

Figure 75 Set GPS based date & time format and time zone via Plant Properties

Plant Properties

Plant name : ID plant

Database path : D:\Documents and Settings\

Plant wide properties

Symbol library : Landscape

Degree type : degrees Celsius

Date format : yyymmdd

Time zone : (GMT+01:00) Amsterdam

Honeywell | Customer | Plant

Name : Honeywell

Street : Industrial Solutions

City :

Country :

Zip Code :

OK Cancel Help

Synchronization Priorities

If multiple time sources have been configured a user defined priority ranking is adhered to determine a choice between up to 3 available time sources as shown in Figure 76 on page 335.

This means that clock synchronization signals from sources of a lower priority will be *ignored* as long as a higher priority source is available.

To determine the validity of available clock sources a time-out protocol is used:

- If a valid time synchronization signal could not be processed within the time-out time set for a particular clock source, that clock source is regarded as temporarily unavailable.

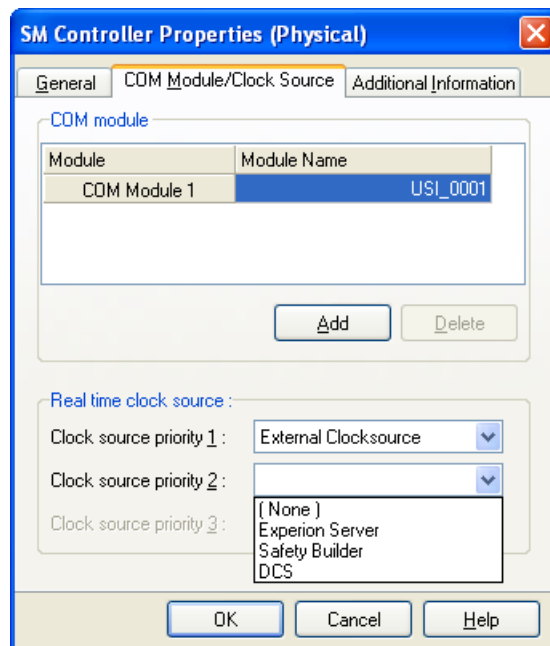
**Note:**

In a network configuration you should consider using the same clock sources and clock source ranking *for all slaves in the network*.

This causes a single master to determine the network time and prevents slave systems to drift apart as a result of using different clock sources in different parts of the network.

Figure 76 on page 335 shows how you can set the clock source priorities from up to 3 different clock sources via the **SM Controller Properties (Physical)** window of **Network Configurator**.

Figure 76 Setting the clock source ranking priority



PTP/NTP based time servers

PTP/NTP based time servers are commercially available.

They are often presented as GPS based time servers supporting the Ethernet Precision Time Protocol (PTP/IEEE 1588) and/or the Network Time Protocols (Safety Manager supports NTP3 and NTP4).

Safety Manager identifies a PTP/NTP based time server as an **External Clock Source** in Network Configurator.



Tip:

To configure time synchronization based on an external PTP or NTP clock source, you use Network Configurator to access the:

1. **External clock source properties** window to set time server details. (See “External Clocksource properties” on page 88 for details.)
 2. **Plant properties** to set the required time zone and format. (See “Plant properties” on page 72 for details.)
-



Attention:

- The accuracy of the PTP based time synchronization signal is 10 milliseconds.
- The accuracy of the NTP based time synchronization signal is 100 milliseconds.
- Experion servers acting as (S)NTP servers are supported by the NTP protocol (For more see “Setting time synchronization in Experion environments” on page 341.)

Possible network delays are compensated.

Each Safety Manager with an Ethernet link to an external clock source can synchronize its real-time clock with the PTP/NTP based time server.

If the PTP/NTP based time server is no longer available, a configured time-out will be initiated.

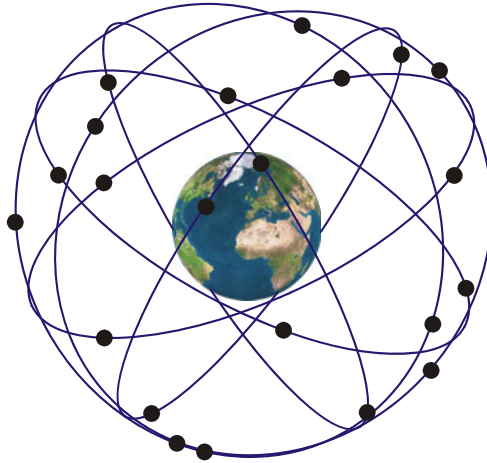
- If the availability recovers before the time-out expires, Safety Manager will continue to use the PTP or NTP signals from the external clock source.
- If the availability does not recover before the time-out expires, Safety Manager will *switch to an alternative time source*.

Time synchronization commands from an external clock source are accepted if the external clock source is regarded as the highest ranked *available* clock source.

About GPS

The GPS (Global-Positioning-System) is a constellation of 24 satellites, arranged in six different orbital planes, each inclined 55 degrees to the equator, as shown in Figure 77 on page 337.

Figure 77 GPS is a constellation of 24 satellites orbiting the sky



Each GPS satellite has an atomic clock and a radio transmitter on-board and transmits a Coordinated Universal Time (UTC) time signal back to earth. A GPS receiver on earth determines its exact location and the local time by analyzing the signals from various GPS satellites.

SafeNet



Tip:

To activate time synchronization by SafeNet:

- Create a logical connection to the network (time) master,
- Add the time master as ranked clock source in the **SM Controller Properties (Physical)**, as described in “SM Controller properties (physical) - tab: Clock Source” on page 82.



Attention:

1. The accuracy of the SafeNet based time synchronization signal is 10 milliseconds per logical connection. Possible network delays are compensated.
2. SafeNet time synchronization signals have no time-out. This means that **Safety Manager will not address lower ranked clock synchronization sources.**
3. If system clocks in a SafeNet configuration drift apart for more than 10 seconds, certain SafeNet commands, such as remote reset, will not function.

When synchronizing via SafeNet a logically connected master is selected as clock source. This master is then referred to as “time master”.

The time master must in term be synchronized by another clock source such as:

- Another SafeNet master (for more information see “Master/slave” on page 319.)
- PTP/NTP based time servers
- Experion server
- A Modbus device
- Safety Station

Time synchronization via SafeNet is based on:

- the PTP protocol when running on top of an Ethernet layer,
- a proprietary protocol when running on top of conventional serial layers.

Time master



Note:

In a network configuration you should consider using the same clock sources and clock source ranking *for all slaves in the network*.

This causes a single master to determine the network time and prevents slave systems to drift apart as a result of using different clock sources in different parts of the network.

The Safety Manager time master is Safety Manager in the SafeNet network that is at the top of the network hierarchy. It obtains time information from its clock sources, and issues time synchronization commands to the other Safety Managers in the network. This is done at least once within the defined SafeNet time-out interval. For more information see “Protocol versus response time” on page 324.

In a SafeNet configuration you must rank the network master as priority 1 for the slave Safety Managers and have all slaves use the same clock sources and ranking order. This to avoid the various system clocks in a network to drift apart.

Experion server



Tip:

To activate time synchronization by Experion

- Set ***Clock Source allowed*** in the **Experion properties** window, as described in “Experion server properties” on page 86.
- Add the Experion server as ranked clock source in the **SM Controller Properties (Physical)**, as described in “SM Controller properties (physical) - tab: Clock Source” on page 82.

See also “Setting time synchronization in Experion environments” on page 341.



Attention:

The accuracy of the Experion time synchronization signal is 1 second + network delay. Network delays are *not* compensated.

A connected Experion[™] server can be configured to send time synchronization commands automatically in fixed (configurable) intervals, or the user can send them manually.

Time synchronization commands from an Experion server are accepted if the Experion server is regarded as the highest ranked *available* clock source.

After a time synchronization command from Experion is accepted, a 26 hour time-out is initiated per default. Experion is regarded faulty for time synchronization if no new time synchronization command is received within these 26 hours (default). During this time-out period, Safety Manager will ignore time synchronization data from sources of lower priority (see “Synchronization Priorities” on page 334 for details).

As soon as the time-out expires without a new time synchronization command having been received, the Safety Manager network will accept time synchronization commands from a lower-level source.

Modbus



Tip:

To activate time synchronization by Modbus

- Set ***Clock Source allowed*** in the **DCS properties** window, as described in “DCS properties” on page 87.
 - Add the Modbus device as ranked clock source in the **SM Controller Properties (Physical)**, as described in “SM Controller properties (physical) - tab: Clock Source” on page 82.
-



Attention:

The accuracy of the Modbus time synchronization signal is 1 second + network delay. Network delays are *not* compensated.

Certain Modbus devices can be configured to send time synchronization commands manually, or automatically in fixed (configurable) intervals. For details see the user guide of the Modbus device.

Time synchronization commands from the Modbus device are accepted if the Modbus device is regarded as the highest ranked *available* clock source.

You must choose an appropriate time-out setting for the clock source update frequency; this may vary per Modbus device.

The Modbus device is regarded faulty for time synchronization if no new time synchronization command is received within the time-out period. During this time-out period, Safety Manager will ignore time synchronization data from sources of lower priority (see “Synchronization Priorities” on page 334 for details).

As soon as the time-out expires without a new time synchronization command being received, the Safety Manager network will accept time synchronization commands from a lower-level source.

Safety Station



Tip:

To activate time synchronization by the Safety Station

- Set **Clock Source allowed** in the **Safety Builder properties** window, as described in “Safety Builder properties” on page 74.
- Add the Safety Station as *lowest* ranked clock source in the **SM Controller Properties (Physical)**, for details see “SM Controller properties (physical) - tab: Clock Source” on page 82.



Attention:

1. The accuracy of the Safety Station time synchronization signal is 1 second + network delay. Network delays are *not* compensated.
2. Safety Station time synchronization signals have no time-out. This means that **Safety Manager will not address lower ranked clock synchronization sources.**

A Safety Station can be used to manually send time synchronization commands.

When sending a time synchronization command via the Safety Station *the time zone and time format as set in Windows will be applied by Safety Manager.*

Time synchronization commands from a Safety Station are accepted if the Safety Station is regarded as the highest ranked *available* clock source.

- Time-out mechanisms are disabled when synchronizing via a Safety Station
- To manually synchronize the real time clock of Safety Manager:
 - a. Connect to the SM Controller to synchronize
 - b. Press the synchronize button in Controller Management.

Setting time synchronization in Experion environments



Tips:

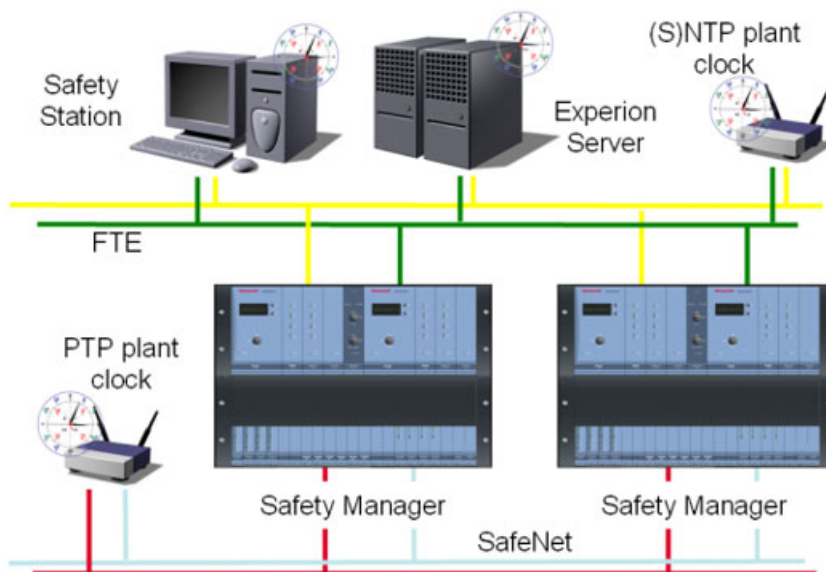
For more information:

- see the hints and tips as described in the *Experion Safety Manager Integration Guide*. You will find this guide on the Experion Knowledge Builder.
- Honeywell provides dedicated training sessions related to time synchronization within Experion.

Figure 78 on page 342 shows that several options for time synchronization become available when as Safety Manager is connected to the Experion™ FTE network.

Which clocks to select and how to rank these depends on the plant setup and philosophy.

Figure 78 Available synchronization devices within an Experion environment



Here are some considerations:

- When both Experion server and an (S)NTP time server are active on FTE, let the (S)NTP synchronization protocol prevail over Experion server protocol:
 - The (S)NTP synchronization protocol provides the best accuracy.
 - If you have SafeNet, synchronize the SafeNet time master with the secondary (S)NTP time server and configure this time master as backup clock source for the SafeNet slave SM Controllers (which individually sync with the primary (S)NTP time server): In the unlikely event that the primary (S)NTP connection over FTE should fail the secondary remains available via the PTP protocol running on SafeNet.
- When you have both CEE controllers and Safety Managers active on FTE, you should realize that process upsets will cause both CEE controller and Safety Manager to generate events.

It is therefore important that both systems sync with the same clock source to keep time stamping of events in CEE controller and Safety Manager remain synchronized with each other. When both systems sync with different clock

sources clocks might drift – as one system maintains a more accurate time than the other due to an inaccuracy or unavailability of the other's clock source.

- When CEE controllers, Safety Managers and Experion serves coexist on the same FTE, synchronizing all systems to the same clock source should prevail over synchronizing to different but more exact clock sources.

FLD symbols

B

APPENDIX

This section gives an overview of the symbols that can be used in FLDs. The table below lists the categories and where more information can be found.

| Symbol set Application Editor | See |
|----------------------------------|----------|
| Connection lines | page 346 |
| IO symbols | page 347 |
| Sheet transfers | page 351 |
| Logical functions | page 353 |
| Compare functions | page 356 |
| Calculation functions | page 358 |
| Mathematical functions | page 360 |
| Counters and registers | page 362 |
| Constants and signal conversions | page 365 |
| Function and equation blocks | page 367 |
| Timers | page 371 |
| Time functions details | page 375 |
| Flip-flops | page 378 |
| Non-functional symbols | page 380 |

Connection lines

Connection lines connect two components to each other. They can be drawn vertically or horizontally. When lines cross, they are not connected. The Application Editor automatically makes a break in the vertical line. However when lines intersect, they are connected. In that case the line is split into two parts at the connection point, unless the connection is made at an end point of the line.

Single line

A single line represents boolean signal.



Double line

A double line represents a binary signal.



IO symbols

Every IO symbol is attached to a point. Points are values that can be read or written by a Control Processor. They usually represent hardware items such as sensors and valves.

Digital input

Digital inputs feed in

- field states such as on/off or start/stop,
- system markers such as CP fault alarm markers



Binary input

Binary inputs feed in:

- binary values such as set points,
- system registers such as remaining repair time.



T is either:

- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits for variables with location “COM” or “FSC”)

Analog input

The analog input feeds the input signal to an A/D converter. The output of the A/D converter is a floating-point binary signal.



Diagnostic input

A diagnostic input can be tied to a point to provide channel and loop status information. Table 22 on page 348 indicates the available diagnostic options.

For more information see “Diagnostic inputs” on page 387.



Table 22 Diagnostic inputs (health status)

| Diagnostic type | Description |
|-----------------|---|
| Channel AND | High when all running Control Processors diagnose the channel as healthy. |
| Channel OR | High when at least one running Control Processor diagnoses the channel as healthy. |
| Loop AND | High when all running Control Processors detect <i>no</i> loop faults (no shorts and no open loops) on the channel. |
| Open Loop AND | High when all running Control Processors detect <i>no</i> open loop fault on the channel. |
| Open Loop OR | High when at least one running Control Processor detects <i>no</i> open loop fault on the channel. |
| Short AND | High when all running Control Processors detect <i>no</i> short on the channel. |
| Short OR | High when at least one running Control Processor detects <i>no</i> short on the channel. |

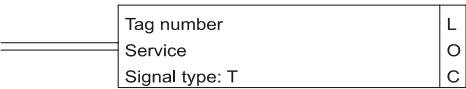
Digital output

Digital outputs feed out boolean values such as start/stop or running/stopped.



Binary output

Binary outputs feed out binary values.

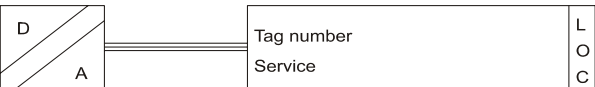


T is either:

- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits for variables with location “COM” or “FSC”)

Analog output

The analog output feeds out the output signal of a D/A converter. The input of the D/A converter is a binary floating-point signal.



Important

Driving a value outside the specified range of 0-20mA of the analog output causes a system shutdown!

Function block boolean input

This is an input in a function block FLD to feed in a boolean signal. See “Function and equation blocks” on page 367.



Function block binary input

This is an input in a function block FLD to feed in a binary signal. See “Function and equation blocks” on page 367.



Function block boolean output

This is an output in a function block FLD to feed out a boolean signal. See “Function and equation blocks” on page 367.



Function block binary output

This is an output in a function block FLD to feed out a binary signal. See “Function and equation blocks” on page 367.



Sheet transfers

Sheet transfers interconnect signals between different FLDs when a function requires more than one FLD. A sheet transfer contains information about the originating FLD and the destination FLD. A sheet transfer also has a sequence number to distinguish it from other sheet transfers between the two FLDs.

Boolean on-sheet transfer

This transfer receives a boolean signal from another FLD.



Binary on-sheet transfer

This transfer receives a binary signal from another FLD.

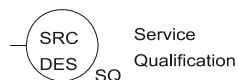


T is either:

- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits)

Boolean off-sheet transfer

This transfer routes a boolean signal to another FLD.



Binary off-sheet transfer

This transfer routes a binary signal to another FLD.

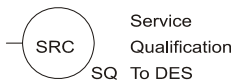


T is either:

- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits)

Multiple boolean off-sheet transfer

This transfer routes a boolean signal to maximal five other FLDs.



Multiple binary off-sheet transfer

This transfer routes a binary signal to maximal five other FLDs.



T is either:

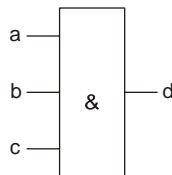
- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits)

Logical functions

Logical functions are basic building blocks to realize the logic of a function in FLDs.

AND

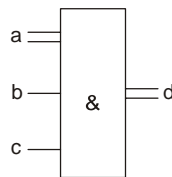
The AND symbol can be used as a logical gate and as a filter. The AND filter passes through a binary value when the filter conditions are all true. If one of them is false, the binary output value is zero.



AND gate

Function:

$$d = a \cdot b \cdot c$$



AND filter

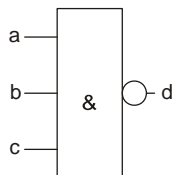
Function:

$$b \cdot c = 1 \Rightarrow d = a$$

$$b \cdot c = 0 \Rightarrow d = 0$$

The symbol height of the AND function can be changed. The maximum number of boolean inputs is 26.

NAND gate

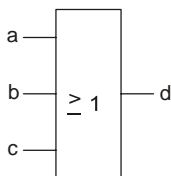


Function:

$$d = \neg(a \cdot b \cdot c)$$

The symbol height of the NAND gate can be changed. The maximum number of boolean inputs is 26.

OR gate

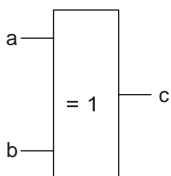


Function:

$$d = a + b + c$$

The symbol height of the OR gate can be changed. The maximum number of boolean inputs is 26.

XOR gate

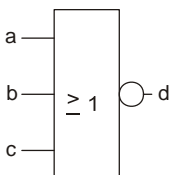


Function:

$$c = (-a) \cdot b + a \cdot (-b)$$

The XOR gate symbol only has two inputs. Its height is fixed.

NOR gate

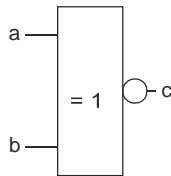


Function:

$$d = -(a + b + c)$$

The symbol height of the NOR gate can be changed. The maximum number of boolean inputs is 26.

XNOR gate



Function:

$$c = (-a) \cdot (-b) + a \cdot b$$

The XNOR gate symbol only has two inputs. Its height is fixed.

Inverter

An inverter can be placed at the:

- Input of logical functions
- Output of a pulse function
- Output of a timer or a flip-flop
- Set and reset input of a timer or a flip-flop

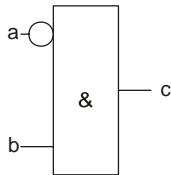


Inverter

Function:

$$b = -a$$

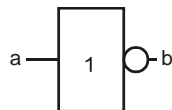
Example of an inverter input



Function:

$$c = (-a) \cdot b$$

Buffer inverter



Function:

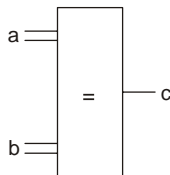
$$b = -a$$

The buffer inverter only has one input. Its height is fixed.

Compare functions

With compare functions you can compare logical states or binary values.

Equal gate



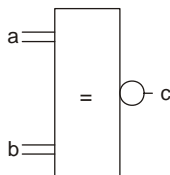
Function:

$$a = b \Rightarrow c = 1$$

$$a \neq b \Rightarrow c = 0$$

The equal gate symbol only has two inputs. Its height is fixed.

Not equal gate



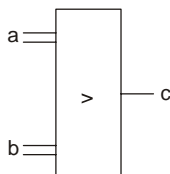
Function:

$$a \neq b \Rightarrow c = 1$$

$$a = b \Rightarrow c = 0$$

The not equal gate symbol only has two inputs. Its height is fixed.

Greater than gate



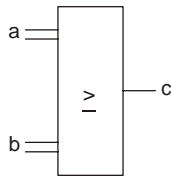
Function:

$$a > b \Rightarrow c = 1$$

$$a \leq b \Rightarrow c = 0$$

The greater than gate symbol only has two inputs. Its height is fixed.

Greater than or equal gate



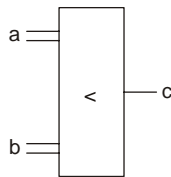
Function:

$$a \geq b \Rightarrow c = 1$$

$$a < b \Rightarrow c = 0$$

The greater than or equal gate symbol only has two inputs. Its height is fixed.

Less than gate



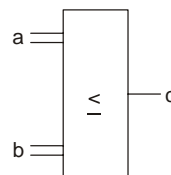
Function:

$$a < b \Rightarrow c = 1$$

$$a \geq b \Rightarrow c = 0$$

The less than gate symbol only has two inputs. Its height is fixed.

Less than or equal gate



Function:

$$a \leq b \Rightarrow c = 1$$

$$a > b \Rightarrow c = 0$$

The less than or equal gate symbol only has two inputs. Its height is fixed.

Calculation functions

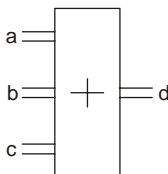
With calculation functions you can perform calculations on binary values.



Important

- Calculations with invalid numbers (for example divide by zero, or square root of negative numbers) or out of range results of the chosen signal type (for example $100 + 73$ is out of range for signal type byte) cause a system shutdown.
 - If an overflow of a binary code decimal (BCD) signal occurs, it is clamped to its maximum value.
-

Addition gate

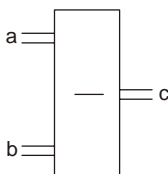


Function:

$$d = a + b + c$$

The symbol height of the addition gate can be changed. The maximum number of binary inputs is 26.

Subtract gate

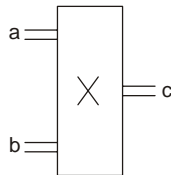


Function:

$$c = a - b$$

The subtract gate symbol only has two inputs. Its height is fixed.

Multiply gate

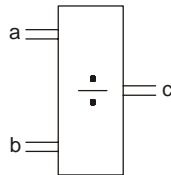


Function:

$$c = a \times b$$

The multiply gate symbol only has two inputs. Its height is fixed.

Divide gate



Function:

$$c = a \div b$$

The divide gate symbol only has two inputs. Its height is fixed.

For floating-point numbers a floating-point division method is used while for byte/word/long numbers, an integer division method is used which truncates the result (for example $16 \div 5 = 3$).




Important

A divide by zero causes a system shutdown!

Mathematical functions

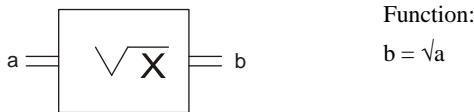
These functions allow you to perform mathematical operations on binary values.




Important

- Calculations with invalid numbers (for example divide by zero, or square root of negative numbers) or out of range results of the chosen signal type (for example $100 + 73$ is out of range for signal type byte) cause a system shutdown.
- If an overflow of a binary code decimal (BCD) signal occurs, it is clamped to its maximum value.

Square root gate



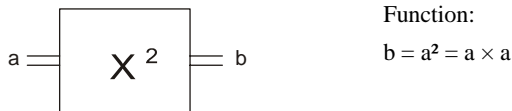
The square root gate symbol only has one input. Its height is fixed.
This gate always produces a floating-point result.



Important

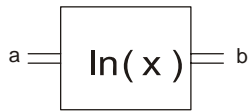
A square root gate with a negative operand causes a system shutdown!

Square gate



The square gate symbol only has one input. Its height is fixed.
This gate always produces a floating-point result.

Natural logarithm gate



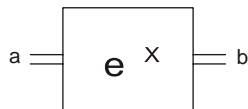
Function:

$$b = \ln(a)$$

The natural logarithm gate symbol only has one input. Its height is fixed.

This gate always produces a floating-point result.

Exponent gate



Function:

$$b = e^a$$

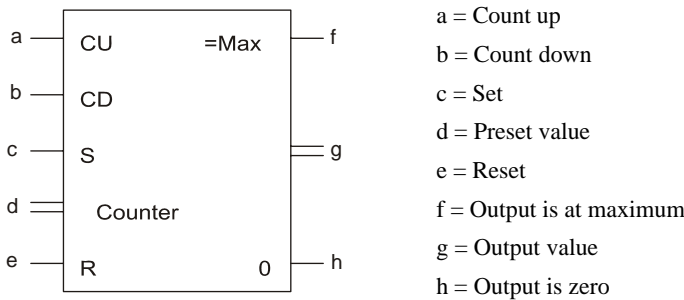
The exponent gate symbol only has one input. Its height is fixed.

This gate always produces a floating-point result.

Counters and registers

With counters and registers you can count events and store binary values.

Counter



Important
Loading a value outside the specified range of 1 to 8191 in the counter causes a system shutdown!

All input and output signal types are specified in the symbol. Its height is fixed.
Output f becomes true when the counter reaches the maximum counter value ($1 \leq \text{Max} \leq 8191$). If the counter has reached the maximum value, its output becomes zero on the next count up.

Function:

| | a | b | c | d | e | f | g | h |
|------------|---|---|---|-----------------|---|-----------------|-------|-----------------|
| Reset | – | – | – | – | 1 | 0 | 0 | 1 |
| Set | – | – | 1 | x ⁴⁾ | 0 | – ¹⁾ | x | – ²⁾ |
| No change | – | – | 0 | – | 0 | f ³⁾ | g | h ³⁾ |
| Count down | 0 | 1 | 0 | – | 0 | 0 | g – 1 | 0 |
| Count up | 1 | 0 | 0 | – | 0 | 0 | g + 1 | 0 |

| (continued) | a | b | c | d | e | f | g | h |
|---|---|---|---|---|---|---|---|---|
| <p>– = value is do not care.</p> <p>1) If $x = \text{Max}$, then $f = 1$; else $f = 0$.</p> <p>2) If $x = 0$, then $h = 1$; else $h = 0$.</p> <p>3) If $g = 0$, then $h = 1$; else $h = 0$. If $g = \text{Max}$, then $f = 1$; else $f = 0$.</p> <p>4) If $x < 0$ or $x > \text{Max}$, then trip.</p> | | | | | | | | |

The inputs CU and CD count on the leading edge of the connected signal. Valid input combinations are:

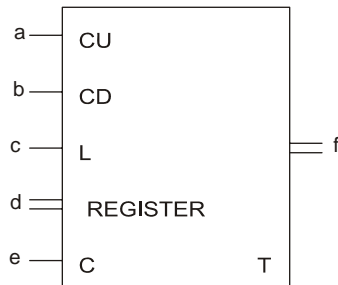
- Set and value
- Count up
- Count down

In these cases the other signals have no effect. The maximum number of counters per FLD is 32. The maximum number of counters per application is 510.

Register

A register can be used as a:

- Storage element of intermediate calculation results
- Memory element for numbers
- Counter for large numbers



a = Count up

b = Count down

c = Load

d = Preset register value

e = Clear

f = Register output value

T is either:

- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits)

All input and output signal types are specified in the symbol. Its height is fixed.

Function:

| | a | b | c | d | e | f | |
|---------------------------|---|---|---|---|---|---------|----------------|
| Clear | – | – | – | x | 1 | 0 | |
| Load | – | – | 1 | y | 0 | y | |
| Unchanged | – | – | 0 | v | 0 | x | |
| Count down | 0 | 1 | 0 | f | 0 | $f - 1$ | (every cycle)* |
| Count up | 1 | 0 | 0 | f | 0 | $f + 1$ | (every cycle)* |
| – = value is do not care. | | | | | | | |

* The output value is set to zero when exceeding a count limit of the register (up or down). The count limits depend on the type of signal chosen for counting (Byte, Word or Long).

When high, the inputs CU and CD count once per program cycle. A pulse gate in the count signal can be used to prevent that CU or CD counts every program cycle.

The CU and CD inputs of a floating-point register can not be used and must remain open. Valid input combinations are:

- Load and value
- Count up, load and value
- Count up and clear
- Count down, load and value
- Count down and clear

In these cases the other signals have no effect. The maximum number of registers per FLD is 32.

Constants and signal conversions

You can use these symbols to enter constant values and perform signal conversions in FLDs.

Constant value

This type of symbol allows you to enter a constant value in a FLD. Its value is fixed and is fixed by the application.

| | |
|---|-------|
| T | VALUE |
|---|-------|

Constant value

T is either:

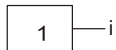
- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits)

The height of the symbol is fixed.

The range of constant value depends on the signal type:

| Type | Range |
|------|--|
| B | −128 to +127 |
| W | −32,768 to +32,767 |
| L | −2,147,483,648 to +2,147,483,647 |
| F | −10 ³⁸ to +10 ³⁸ |

Constant boolean



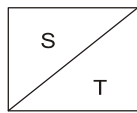
Function:

$i = 1$

Only one input can be connected to the output of this symbol. Its height is fixed.

Signal conversion

This function converts a signal to another format.



Converts signal S to type T

S and T are either:

- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits)

The converter function checks if the value of the input symbol is within the range of the type T.

Only downward conversions are allowed (see table below).

| | Target (Output) | | | |
|----------------|-----------------|-----|-----|----|
| Source (Input) | B | W | L | F |
| B | – | No | No | No |
| W | Yes | – | No | No |
| L | Yes | Yes | – | No |
| F | Yes | Yes | Yes | – |
| – trivial | | | | |

Important

A system shutdown occurs when:

- The input value is out of range and causes a calculation overflow.

Function and equation blocks

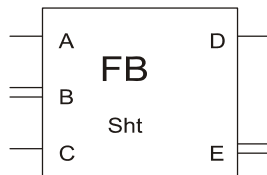
For more information about function and equation blocks, see “Function and equation blocks” on page 209.

Function block

A function block is a subroutine whose logic is created on another FLD (of block type function block). This function block FLD must have a higher sheet number than the FLD in which it is used, and the sheet number of the function block FLD must be 500 or higher.

When a function block is placed on an FLD, the function block FLD sheet number is used as a reference to the function block.

A function block has no system outputs and no off-sheet references. It has function block inputs and outputs to transfer values to and from the FLD that uses the function block within its logic.



A, B, C, D and E are of the type:

- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits)

Please note that the number of inputs and outputs can be different for each function block.

At least one output must be connected. All connected signals must be of a compatible type. For example, signals of type byte can be connected to byte, word or float inputs.

Function block inputs and outputs can only be used on function block FLDs.

Function block inputs represent the signals entering the function block, and Function block outputs represent the signals leaving the function block.



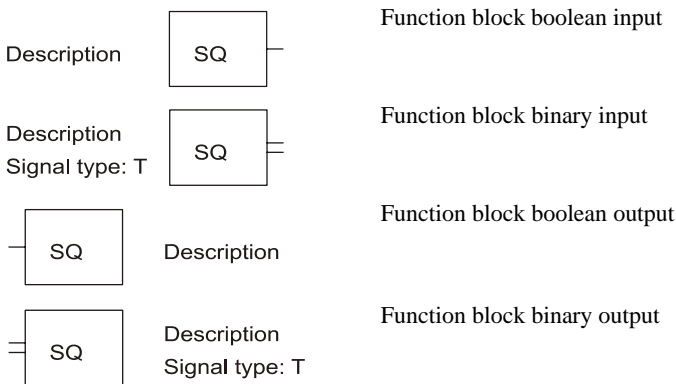
Attention:


In some occasions changes to the function block input and output *properties* are not automatically updated on the FLDs that call the function block.

To update you must:

1. Right-click the function block in each FLD and select *change* from the pop-up menu.
2. Reselect the function block to refresh its properties on the FLD
3. do this for every FLD containing the function block

They are essentially different from Safety Manager inputs and outputs. The function block inputs and outputs can be boolean and binary. Boolean inputs and outputs are represented by single lines, and binary inputs and outputs by double lines.





Note

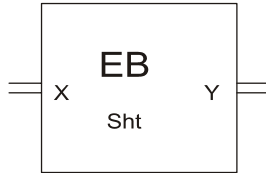
- The function block sheet number must be higher than the sheet number of the FLD in which the function block is used.
- The function block sheet number must be 500 or higher.
- Once a function block FLD has been drawn, the FLDs with higher sheet numbers can only be equation blocks or function blocks.

Equation block

An equation block is a subroutine that uses a binary input value to calculate a binary output value (floating point) using an equation table. The equation table is entered in another FLD (of block type equation block).

This equation block FLD must have a higher sheet number than the FLD in which it is used, and the sheet number of the equation block FLD must be 500 or higher.

When an equation block is placed on an FLD, the equation block FLD sheet number is used as a reference to the equation block.



X can be of the type:

- B (Byte, 8 bits)
- W (Word, 16 bits)
- L (Long, 32 bits)
- F (Floating point, 32 bits)

Y is always of the type F (Floating point, 32 bits).

An equation block symbol can be used to approximate complex calculations. Logarithmic, exponential, differential functions, and so on can be approximated with an approximation table. In Table 23 on page 369 you find an example of a square approximation table for values between 0 and 5.

An equation block exists only when the equation table is successfully loaded. Once you have defined an equation table in an equation block FLD, the equation block can be used in an FLD with a lower FLD sheet number.

The input (**x**) and the output (**y**) must be connected to other symbols.

Table 23 Example of equation function

| | X | Y |
|--|-----|-------|
| | 0 | 0 |
| | 0.5 | 0.25 |
| | 1 | 1 |
| | 1.5 | 2.25 |
| | 2 | 4 |
| | 2.5 | 6.25 |
| | 3 | 9 |
| | 3.5 | 12.25 |
| | 4 | 16 |
| | 4.5 | 20.25 |
| | 5 | 25 |

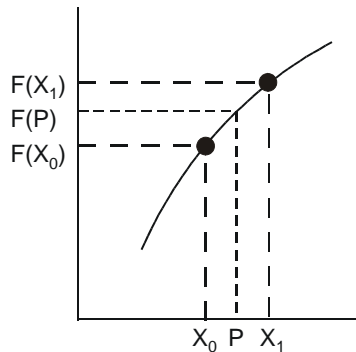
Creating an equation table

For information regarding creation of an equation table see “Creating equation blocks” on page 210.

Execution of an equation block

Safety Manager uses linear interpolation to approximate the output value for an input value that is located between two input values (see Figure 79 on page 370).

Figure 79 Approximating an output value to an input value



The following approximation algorithm is used:

$$f(P) = f(X_0) + \frac{f(X_1) - f(X_0)}{X_1 - X_0}(P - X_0)$$



Note

The input (x) value is clamped on the first and the last value in the equation table. This means that a value smaller than the first input value in the equation table will result in an output value equal to the first output value of the equation table.

Similarly, an input value larger than the last input value in the equation table will result in an output value equal to the last output value of the equation table.

Timers

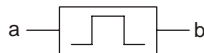
There are two types of time functions:

1. Timers with a variable timer value. The timer value is determined by a binary signal (byte or word) connected to the input of the timer symbol.
2. Timers with a fixed timer value.

See also “Time functions details” on page 375.

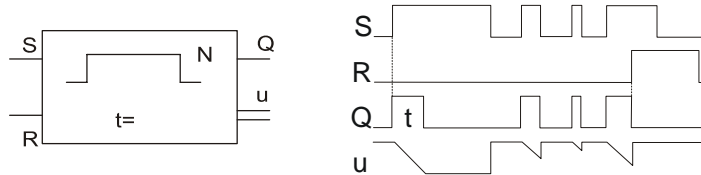
Pulse

This function can be used to generate a pulse with a duration of one application cycle on the leading edge of the input signal (input signal from false to true). To generate a new pulse, the input must become false first.



Timers with constant timer value: pulse

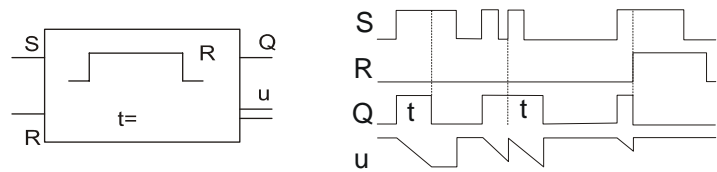
This is a pulse time function which triggers on the leading edge of the set signal.



If only one input is connected, it is assumed to be the set input.

Timers with constant timer value: pulse retriggerable

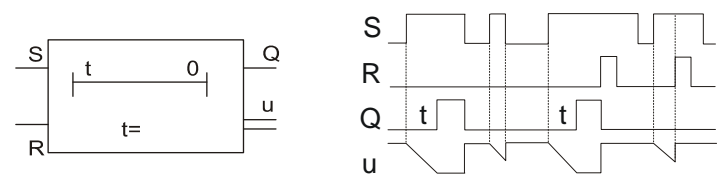
This is a pulse time function which triggers on the leading edge of the set signal. The timer retriggers on each leading edge of the set signal.



If only one input is connected, it is assumed to be the set input.

Timers with constant timer value: delayed on

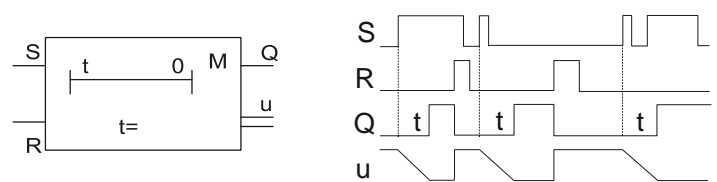
This is a delayed on time function which triggers on the leading edge of the set signal.



If only one input is connected, it is assumed to be the set input.

Timers with constant timer value: delayed on memorize

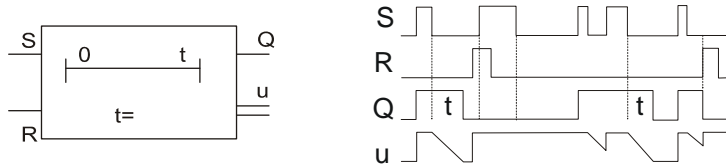
This is a delayed on time function which triggers on the leading edge of the set signal. The timer continues counting when the set signal becomes false again.



All inputs must be connected.

Timers with constant timer value: delayed off

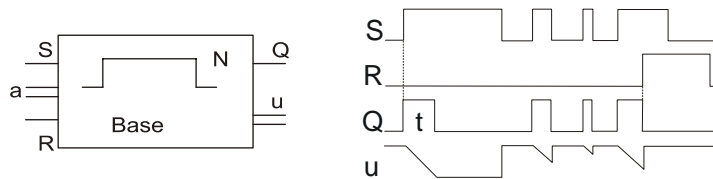
This is a delayed off time function which triggers on the trailing edge of the set signal.



If only one input is connected, it is assumed to be the set input.

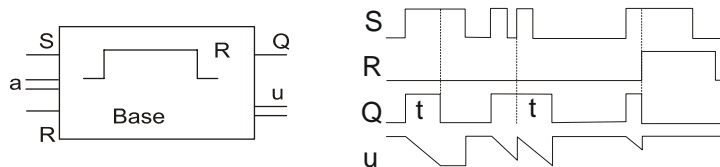
Timers with variable timer value: pulse

This is a pulse time function which triggers on the leading edge of the set signal.



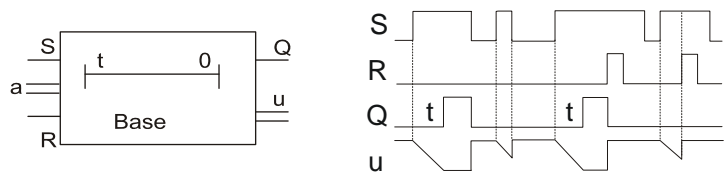
Timers with variable timer value: pulse retriggerable

This is a pulse time function which triggers on the leading edge of the set signal. The timer retriggers on each leading edge of the set signal.



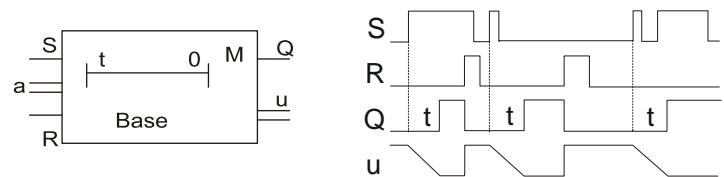
Timers with variable timer value: delayed on

This is a delayed on time function which triggers on the leading edge of the set signal.



Timers with variable timer value: delayed on memorize

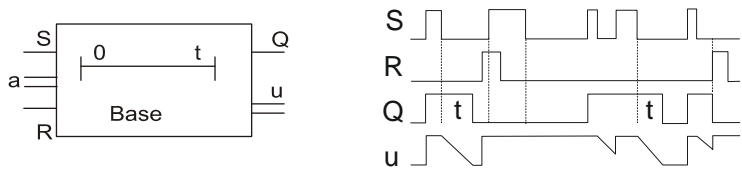
This is a delayed on time function which triggers on the leading edge of the set signal. The timer continues counting when the set signal becomes false again.



All inputs must be connected.

Timers with variable timer value: delayed off

This is a delayed off time function which triggers on the trailing edge of the set signal.



Time functions details

Timer base

The timer base determines the smallest unit of a timer period. The timer duration is a multiple of the timer base. The following timer bases can be selected:

| Base | Granularity |
|-------|------------------|
| 10ms | 10 milliseconds |
| 100ms | 100 milliseconds |
| s | 1 second |
| m | 1 minute |



Note

The base of timers with a variable timer value is fixed. For each timer base, Safety Manager uses a common timer to update the timers with that base.

The base of timers with a fixed timer value may be changed automatically to achieve better accuracy of the timer value (see further on).

Timer value

The period that a timer runs is the timer value times the timer base.

- For timers with a fixed timer value, the timer value is defined in the FLD when the timer is added to the logic.
- For timers with a variable timer value, the timer value is defined by a binary input of the timer.

If the timer base is 100 ms, only integer timer values are allowed. If the timer base is seconds or minutes, you can also use decimal values.

The timer values must be greater than zero. A zero value is changed to the nearest allowed value. The maximum timer value lies in the order of 2^{29} , i.e. $>500+E6$:

To achieve a better timer accuracy, the timer base of timers with a fixed timer value automatically changes depending on the timer value.



Important

Make sure that you do not exceed the maximum timer value; this causes a system shutdown.

Accuracy of timers with a variable timer value

The base of timers with a variable timer value is fixed. For each timer base, Safety Manager uses a common timer to update these timers.

As a result, a timer with a 1m base and value of 1 expires between 1 - 60 s and a timer value of 2 expires between 61 - 120 s and so on. Similarly, a timer with timer base 1s expires between 100 ms and 1 second. It is important that you choose a timer base with the best resolution for the required accuracy.

For example, a 20-minute timer can have a base of:

- m
If the timer uses base “m” and has a timer value of 20, it expires between 19:01 and 20:00 m. The maximum deviation is 59 s, which is 4.91% of the timer value.
- s
If the timer uses base “s” and has a timer value of “1199” (which is 19:59 m), it expires between 1198 and 1199 s. The maximum deviation is 1 s, which is 0.08% of the timer value.

Accuracy of timers with a fixed timer value

The Safety Builder automatically changes the base of timers with a fixed timer value to achieve better timer accuracy.

| Timer base | Timer value [units] | Base changes to |
|------------|---------------------|-----------------|
| m | 0.01 - 10.00 | s |
| | 10.01 - 2027.00 | - |
| s | 0.01 - 10.00 | 100 ms |
| | 10.01 - 1199.00 | - |
| | 1200 - 9999 | m |
| 100ms | 1 - 99 | - |
| 10ms | 1 - 99 | - |

Maximum number of timers

The maximum number of timers in a application depends on the timer base:

| Base | Maximum number of timers |
|-------|--------------------------|
| 10ms | 98 |
| 100ms | 748 |
| s | 748 |
| m | 446 |

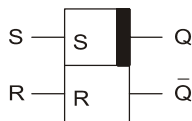
The maximum number of timers per FLD is 32 (including timers in function blocks).

Flip-flops

Flip-flops are logical circuits which retain their logical state even after the controlling input signal has been removed. The two outputs always have opposite logic levels.

S-R Flip-flop

A set-reset flip-flop with a dominant set.



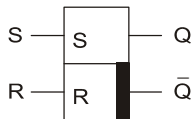
Function:

| S | R | Q | –Q | Remark |
|--|---|--------|------------|-----------------|
| 0 | 1 | 0 | 1 | |
| 1 | 0 | 1 | 0 | |
| 0 | 0 | Qt – 1 | – (Qt – 1) | State unchanged |
| 1 | 1 | 1 | 0 | Set is dominant |
| “Qt – 1” is the state during the previous cycle. | | | | |

All inputs and at least one of the outputs must be connected.

R-S Flip-flop

A reset-set flip-flop with a dominant reset.



Function:

| S | R | Q | \bar{Q} | Remark |
|---|---|-----------|-----------------|-------------------|
| 0 | 1 | 0 | 1 | |
| 1 | 0 | 1 | 0 | |
| 0 | 0 | Q_{t-1} | \bar{Q}_{t-1} | State unchanged |
| 1 | 1 | 0 | 1 | Reset is dominant |
| “ Q_{t-1} ” is the state during the previous cycle. | | | | |

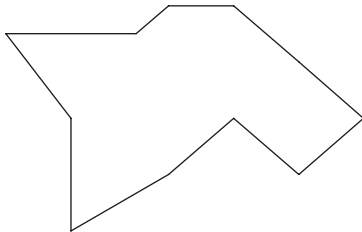
All inputs and at least one of the outputs must be connected.

Non-functional symbols

Non-functional symbols do not contribute to the function of an FLD but help to organize the symbols on the sheet.

Revision clouds

The revision cloud symbol is a polygon with dashed lines. It can be used to identify changed parts.



Texts

You can add explanatory or descriptive text to an FLD. The text consist of a single line with a maximum of 60 characters. You can place the text everywhere even across symbols. The character size is adjustable from 1 through 10.

If the character size is larger than 1, the stroke size can range from 1 up to the character size. The stroke size determines the boldness of the text.

`Text (scale factor 1, no. of strokes 1)`

Text (scale factor 3, no. of strokes 1)

Text (scale factor 3, no. of strokes 3)

Safety Manager system points

C

APPENDIX

Safety Manager has a number of system points that are generated by the system and can be used in the application to indicate an alarm or a state or initiate an action:

- System markers and registers indicate the state of the system,
- Alarm markers indicate the occurrence of an abnormal system state,
- Reset markers allow to remotely reset a slave system,
- Diagnostic inputs indicate the health of the related IO channel or IO loop.
- Applying system points in the application logic (example).

All topics are discussed in this appendix.

| Topic | See |
|--|----------|
| System markers and registers | page 382 |
| Reset markers | page 384 |
| Alarm markers and registers | page 385 |
| Diagnostic inputs | page 387 |
| Diagnostic status exchange with external controllers | page 389 |

System markers and registers

**Tip:**

A number of system marker and register properties can be renamed.

When doing so, it is recommended to leave the tag name unchanged but to modify the description field to better match the actual use.

- For marker ExtComFaultCC1 in Table 14 on page 84 for example, you could change:
 - External communication fault in Experion FTE link.
-

System markers and system registers are used to reflect the system state via the application.

System markers

The following system markers are available:

Table 24 Safety Manager system markers^{*}

| System marker | Description |
|-----------------|-----------------------------|
| #-FaultReset | Fault reset input |
| #-ForceEnable | Force enable |
| #-ClockSync | Clock synchronization input |
| #-CP1_Running | Control Processor 1 running |
| #-CP2_Running | Control Processor 2 running |
| #-ForceActive | IO forced |
| #-Flasher-0.5Hz | 0.5 Hz flasher |
| #-Flasher-1Hz | 1 Hz flasher |
| #-Flasher-2Hz | 2 Hz flasher |
| #-Flasher-5Hz | 5 Hz flasher |

^{*} # Stands for the Controller node number, as defined in "Physical SM Controller properties" on page 75

The following system markers are available after allocation of a channel/module:

Table 25 Diagnostic input markers

| System marker | Description | Available on IO Module |
|-----------------|------------------------|------------------------|
| EFM cab.c/s/ch* | Earth Fault Monitoring | SDIL-1608 |

* cab.c/s/ch stands for cabinet, chassis, slot number and channel of the earth fault.

System registers

The following system registers are available:

Table 26 Safety Manager system registers*

| System register | Description |
|-----------------|---------------------------------|
| #-TempCP1 | Temperature Control Processor 1 |
| #-TempCP2 | Temperature Control Processor 2 |
| #-Second | Second |
| #-Minute | Minute |
| #-Hour | Hour |
| #-Day | Day |
| #-DayOfTheWeek | Day of the week |
| #-Month | Month |
| #-Year | Year |

* # Stands for the Controller node number, as defined in "Physical SM Controller properties" on page 75

The following system registers are available after allocation of a channel/module:

Table 27 Diagnostic input registers

| System marker | Description | Available on IO Module |
|----------------|--------------------|------------------------|
| VM cab.c/s/17* | Voltage Monitoring | SAI-1620 |

* cab.c/s identifies the cabinet, chassis and slot number of the module. 17 is a dedicated channel for Voltage monitoring

Reset markers

Safety Manager masters in a SafeNet network have a reset marker for each logical slave system they control.

A reset marker is an output marker location `SYS`, which is available in the application of SafeNet masters.

- A High state, or 1, applied to the reset marker output causes a remote reset command to be sent by the master system to the slave system that is being addressed.
- The marker is tagged `Fault Reset SM Controller_#`, where # is to be replaced by the system number of the logical slave being addressed.

Preconditions for a slave to accept a remote reset command are:

- The QPP key switch of the slave is in RUN and the slave system is ready to start,
- The real time clock (RTC) of the master and slave system must be in sync.



Notes:

The time difference and time delay between master and slave real time clock (RTC) must be < 10 seconds:

- If a reset command is sent, it is time stamped by the master. When received, this time stamp is compared to the RTC of the slave; if the command appears more than 10 seconds old it is rejected.
- Note that aging of the command is usually caused by network delay.

After a reset command is sent to a slave, all following reset commands for that slave are ignored for the next 20 seconds.

- *The delay timer is restarted each time* a new reset command is received within 20 seconds after the last one.
-

There is one reset marker available per logically connected slave:

- A reset pulse shall last at least one cycle of the master application.
- A reset command is only accepted when received within 10 seconds after time stamping by the master. (See note above)
- Reset commands shall be given at intervals >> 20 seconds. For details see above note.
- Reset markers are controlled by the application in the master.

Alarm markers and registers

Safety Manager uses a number of alarm markers and alarm registers to indicate the occurrence of abnormal system state. Some markers are general markers, others are specific.

Alarm markers

The following alarm markers are available:

#-#-

Table 28 Safety Manager alarm markers^{*}

| Alarm marker | Description |
|---------------------------------|---|
| #-TempHH_Alarm | Temperature high-high alarm |
| #-TempH_Alarm | Temperature high alarm |
| #-TempL_Alarm | Temperature low alarm |
| #-TempLL_Alarm | Temperature low-low alarm |
| #-ExtComFaultCC1 | External communication fault in communication channel 1 |
| #-ExtComFaultCC2 | External communication fault in communication channel 2 |
| #-ExtComFaultCC3 | External communication fault in communication channel 3 |
| #-ExtComFaultCC4 | External communication fault in communication channel 4 |
| #-ExtComFaultCC5 | External communication fault in communication channel 5 |
| #-ExtComFaultCC6 | External communication fault in communication channel 6 |
| #-ExtComFaultCC7 | External communication fault in communication channel 7 |
| #-ExtComFaultCC8 | External communication fault in communication channel 8 |
| #-ClockSrcFault1 | Clock source 1 fault |
| #-ClockSrcFault2 | Clock source 2 fault |
| #-ClockSrcFault3 | Clock source 3 fault |
| #-SecSwitchOff | Secondary switch-off activated |
| #-CP_Fault | Control Processor fault |
| #-ControllerFault ^{**} | Safety Manager Controller fault |
| #-InputFault ^{***} | Input channel fault |
| #-InputLoopFault | Input loop fault |
| #-InputCompare | Input compare fault |
| #-OutputFault ^{****} | Output channel fault |
| #-OutputLoopFault | Output loop fault |
| #-OutputCompare | Output compare fault |

Table 28 Safety Manager alarm markers* (continued)

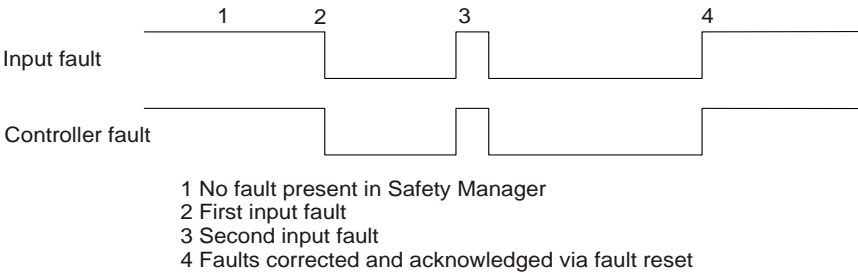
| Alarm marker | Description |
|------------------------|-----------------------------|
| #-RepairTimerStart_CP1 | Repair timer started in CP1 |
| #-RepairTimerStart_CP2 | Repair timer started in CP2 |

- * # Stands for the Controller node number, as defined in "Physical SM Controller properties" on page 75
- ** Turns 0 (fault state) at any type of fault detected
- *** Turns 0 (fault state) at any type of input fault detected
- **** Turns 0 (fault state) at any type of output fault detected

Alarm marker state

The normal state of a marker (no fault detected) is 1. When the first fault is detected, the associated alarm marker changes to 0. Any subsequent fault of the same type causes the alarm marker to pulse for one application program cycle (see Figure 80 on page 386).

Figure 80 Input failure alarm marker function



Remaining repair time

The following registers are available to indicate the remaining repair time:

Table 29 Safety Manager alarm registers

| Repair timer registers | Description |
|------------------------|---|
| Repair_CP1 | Remaining repair time Control Processor 1 |
| Repair_CP2 | Remaining repair time Control Processor 2 |

Diagnostic inputs

Diagnostic inputs are available for every point allocated on a testable IO module.

All diagnostic inputs can be used as a digital input in the functional logic diagrams to indicate the status of the IO.



Note:

A diagnostic input related to health is an application marker, not a (system) point.

Diagnostic inputs can be accessed in a functional logic diagram (FLD) by selecting a diagnostic input as shown in Figure 81 on page 387.

Figure 81 Diagnostic input health indicator

| | |
|---|----------------|
| S | I/O type: Type |
| Y | Tag number |
| S | "Not faulty" |

If the input status is healthy, its diagnostic input is high. If a fault is detected in the channel, the diagnostic input goes low.

The status of the diagnostic inputs does not depend on the safety relation of the channel.

- Figure 82 on page 387 shows the type of diagnostics that can be selected.
- Table 30 on page 388 explains the meaning of these diagnostic types.

Figure 82 Diagnostic input configuration window

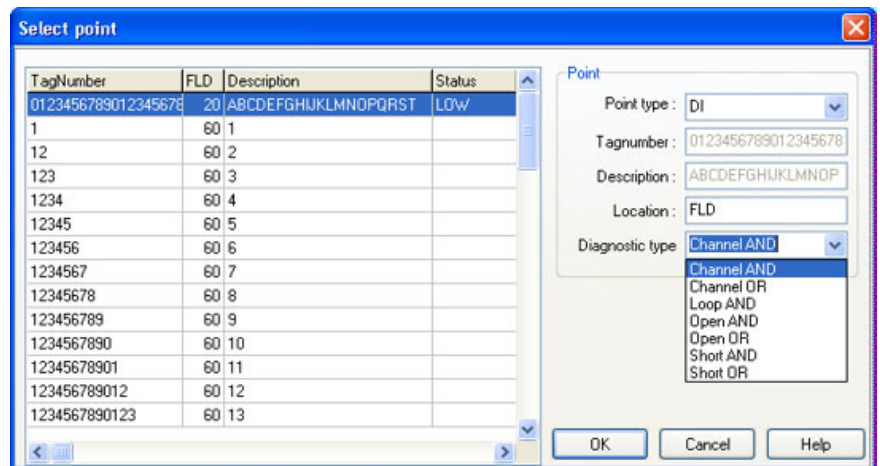


Table 30 Diagnostic inputs (health status)

| Diagnostic type | Description |
|-----------------|---|
| Channel AND | High when all running Control Processors diagnose the channel as healthy. |
| Channel OR | High when at least one running Control Processor diagnoses the channel as healthy. |
| Loop AND | High when all running Control Processors detect <i>no</i> loop faults (no shorts and no open loops) on the channel. |
| Open Loop AND | High when all running Control Processors detect <i>no</i> open loop fault on the channel. |
| Open Loop OR | High when at least one running Control Processor detects <i>no</i> open loop fault on the channel. |
| Short AND | High when all running Control Processors detect <i>no</i> short on the channel. |
| Short OR | High when at least one running Control Processor detects <i>no</i> short on the channel. |

Diagnostic status exchange with external controllers

Safety Manager alarm markers and the diagnostic inputs can be transferred to external controllers to e.g. generate an operator alarm or to initiate a corrective action within the external controller.

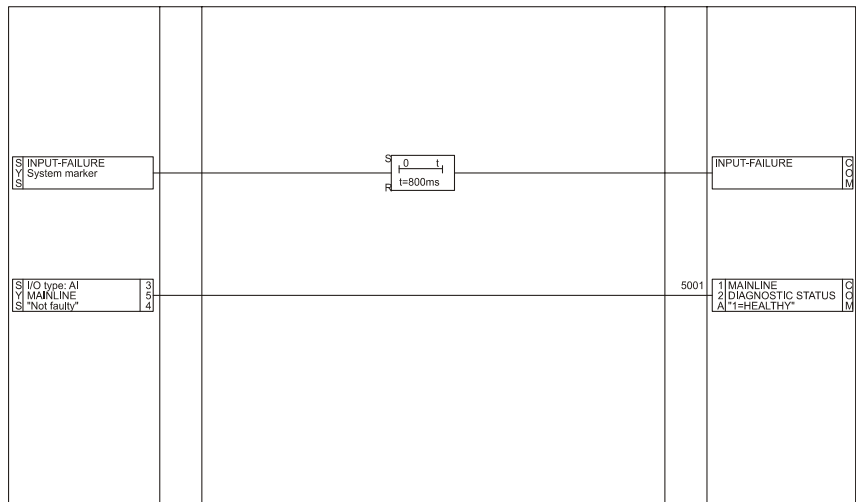


Note

Experion™ PKS can also access diagnostics through dedicated interfaces. See *Overview Guide* for details.

Figure 83 on page 389 shows the functional logic diagram to report the occurrence of an input fault ('InputFault' alarm marker) and the use of a diagnostic input (IO type AI) to report the status of an analog input channel to an external controller.

Figure 83 Safety Manager system information to DCS



The status of the points is transferred to the external controller via outputs with location 'COM', which are allocated to the communication channel to the external controller.

Behavior of alarm markers

The behavior of the alarm markers is quasi-static. Normally, if no fault is present, the value of the markers is high. If a fault is detected, the corresponding alarm

marker becomes low. On subsequent faults the alarm marker becomes high during one application program cycle of Safety Manager (for example 300 ms) and then low again.

If the scan cycle of the external controller lasts longer than the Safety Manager application cycle, it is possible that any subsequent faults are not detected by the external controller. The Safety Manager alarm marker is therefore connected to the output of the external controller via a delayed off timer. Thus, a pulse on the alarm marker is extended to the configured timer value. To ensure detection by the external controller, the timer value must be larger than the external controller scan time.

Behavior of diagnostic inputs

The behavior of the diagnostic inputs is static. Normally, an IO channel is healthy and the value of the corresponding diagnostic input is high. If the IO channel becomes faulty, the diagnostic input becomes low. It remains low until the fault is repaired and a fault reset has been given. The diagnostic input can therefore be connected directly to the output to the external controller.

Point attributes

D

APPENDIX

This section discusses the attributes and parameters of Safety Manager points as stored in the point database.

This section covers the following topics:

| Topic | | See |
|---------------------|----------------|----------|
| Main attributes | | page 393 |
| | Point Type | page 393 |
| | Tag number | page 394 |
| | Description | page 394 |
| | Status | page 394 |
| | Location | page 394 |
| | Unit | page 395 |
| | Subunit | page 395 |
| | SIL | page 395 |
| Detailed attributes | | page 396 |
| | Safety related | page 396 |
| | SOE Enable | page 397 |
| | SOE ID | page 397 |
| | Force enable | page 398 |
| | Write enable | page 399 |
| | Power up | page 399 |
| | Fault reaction | page 399 |
| | Register type | page 400 |
| | Signal type | page 400 |
| | Scaling | page 400 |
| | Bottom scale | page 400 |

| Topic | | See |
|-----------------------|-------------------------------|----------|
| | Top scale | page 401 |
| | Transmitter alarm | page 401 |
| | Eng units (Engineering units) | page 401 |
| Allocation attributes | | page 402 |
| | Size | page 402 |
| | Chassis | page 403 |
| | Slot | page 403 |
| | Channel | page 403 |
| | Communication allocation | page 403 |
| System attributes | | page 407 |
| | FLD number | page 407 |
| | Timer base | page 407 |
| | Timer value | page 408 |
| | Counter range | page 408 |

Main attributes

Main attributes are the most common attributes for points, apart from the allocation attributes.

For details on allocation attributes see “Allocation attributes” on page 402.

The following main attributes can be distinguished:

| Topic | See |
|-------------|----------|
| Point Type | page 393 |
| Tag number | page 394 |
| Description | page 394 |
| Status | page 394 |
| Location | page 394 |
| Unit | page 395 |
| Subunit | page 395 |
| SIL | page 395 |

Point Type

This attribute defines the type of the point.

Table 31 on page 393 lists the point types available in Safety Manager.

Table 31 Safety Manager point types

| Type | Description | |
|------|----------------|---|
| DI | Digital input | Boolean input (either 0 or 1) |
| AI | Analog input | Input with type Long or Float* |
| BI | Binary input | Input with type Byte, Word, Long or Float* |
| DO | Digital output | Boolean output (either 0 or 1) |
| AO | Analog output | Output with type Long or Float* |
| BO | Binary output | Output with type Byte, Word, Long or Float* |
| M | Marker | Boolean |
| C | Counter | Word (range 0 - 8191) |
| T | Timer | Timebase ms, s, min |
| R | Register | Byte, Word, Long or Float* |

- * For an explanation of the register types (Byte, Word, Long, Float) see “Register type” on page 400.

Tag number

The Tag number is the name of a point.

Safety Builder only accepts a point type and tag number combination once. This way, any Safety Manager point is uniquely identified by its type and tag number combination.

- Tag numbers may contain any ASCII characters *except* spaces (' '), semicolons (;), commas (,), asterisk (“*”) and question marks (?).
- The maximum length of a tag number is 32 characters.
- Tag numbers are case-sensitive, which means that e.g. “Test” is not the same as “TEST”.

Description

Here, you can enter point-specific information. The text you enter here does not influence the functioning of Safety Manager. The maximum length of a description is 64 characters.

Status

This field applies to digital points.

It provides a description of the field status when the point value is 1 or high. (A 1 could e.g. stand for High pressure). Such description can be used by SOE devices to provide extra information besides the actual point status.

Location

The location attribute provides information about how the point is used in the application. The location is indicated by a three-character abbreviation which can be defined by the user (for example, you can use FLD when a point is related to a sensor or actuator in the field).

Safety Manager has a number of locations that have a special meaning:

- **ANN:**
Means that the point is related to an alarm function (DI, DO). This location has been reserved for future use.

- **COM:**
Means that the point will be allocated on a logical connection to other devices, *except on logical connections to other SM Controllers*.
 - Points with location COM can be forced
 - Input points with location COM can be written
- **FSC:**
Means that the point will be allocated on a logical connection based on SafeNet which connects to another SM Controller.
 - Points with location FSC are dedicated for SafeNet
 - Input points with location FSC cannot be written
 - Output points with location FSC cannot be forced
- **SYS:**
Means that the point is a system point (reserved for use by Safety Manager programs).

Unit

The unit attribute specifies the name of the unit for which this point is used in the application program, for example F-210 (Furnace 210). The maximum length is 8 characters.

Subunit

The subunit attribute specifies the name of the subunit for which this point is used in the application program, for example B-210 (Burner on Furnace 210). The maximum length is 8 characters.

SIL

Safety Integrity Level. For more information, see “Safety Manager Glossary” on page 519.

Detailed attributes

Detailed attributes are attributes that do not require to be filled as they have a default value.

Nevertheless, in many cases it may be desired to change the default values to your preferences.

The following detailed attributes can be distinguished:

| Topic | See |
|-------------------------------|----------|
| Safety related | page 396 |
| SOE Enable | page 397 |
| SOE ID | page 397 |
| Force enable | page 398 |
| Write enable | page 399 |
| Power up | page 399 |
| Fault reaction | page 399 |
| Register type | page 400 |
| Signal type | page 400 |
| Scaling | page 400 |
| Bottom scale | page 400 |
| Top scale | page 401 |
| Transmitter alarm | page 401 |
| Eng units (Engineering units) | page 401 |

Safety related

**Caution:**

This attribute does *NOT* modify functionality or safety settings of the configuration but exists for reporting purposes only.

This attribute specifies if a point is safety related. Safety related points appear in red in the FLDs.

The fault reaction, as described in “Fault reaction” on page 399, defines the action to be taken in case of a hardware fault on the IO module or the IO channel which the point is allocated to.

SOE Enable

This attribute specifies for each point whether it is enabled or disabled for sequence of event recording.

For details about sequence of event see “Sequence of events (SOE)” on page 441.

SOE ID

This attribute specifies the SOE ID number allocated to the SOE-enabled point.

A SOE ID is allocated automatically when enabling SOE for that point. Use Point Configurator or **import** function to allocate user specific values.

For details about SOE ID's see “Sequence-of-Event Recording to Experion” on page 444.

SOE Setpoint

This attribute is in use with analog points related to SOE.

An event occurs for analog Point types such as AI and AO if the Point application value moves from one operational area to another.

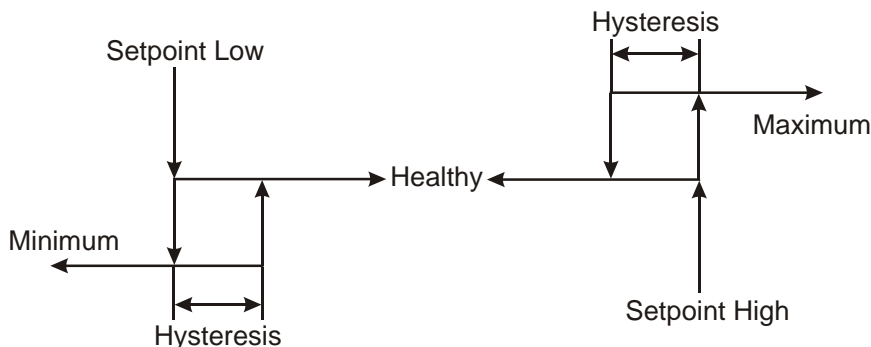
Operational areas

Three operational areas can be defined for analog Points:

1. **Healthy**: this is the normal operational area, between the SOE set point `Low` and the SOE set point `High`,
2. **Low**: This is the low-level alarm area, below the SOE set point `Low`,
3. **High**: This is the high-level alarm area, above the SOE set point `High`.

Figure 84 on page 398 shows the operational areas defined for event recording of Point types AI and AO.

Figure 84 Event definition for Point types AI and AO



Hysteresis

The hysteresis (i.e. "lag") is 0.5% of the full scale of the analog value.

The absolute value of the hysteresis in engineering units depends on the configuration of the Point and can be calculated.

To calculate the hysteresis in engineering units for channels ranging 0-20 mA, 0-5 V or 0-10 V, the following equation is used:

$$\text{hysteresis}_{0-20} = \frac{10 \times (\text{top} - \text{bottom})}{1638} \quad [\text{engineering units}]$$

To calculate the hysteresis in engineering units for channels ranging 4-20 mA, 1-5 V or 2-10 V, the following equation is used:

$$\text{hysteresis}_{4-20} = \frac{20 \times (\text{top} - \text{bottom})}{2621} \quad [\text{engineering units}]$$

Force enable

This attribute specifies for each point whether it is possible to force the point (set it to a certain fixed state). IO points and on-sheet references can both be forced. The "forced" value remains valid until the point force is disabled. All forces are controlled by a *force enable* input (IO-FORCED). Forces are only accepted if the force enable input is high and the *force enable* flag is TRUE. Forces are cleared if the *force enable* input is low.

Write enable

This attribute specifies for each point whether it is possible to write a point. This means the value assigned to the point is overwritten in the next program cycle (unless the point is an input with location COM or FSC).

Power up

In certain situations, it cannot be guaranteed that the variable value is read on power up before it is actually used in the application.

The power up value ensures that a predefined value is applied (e.g. during power up of the system) until a scanned or calculated IO value can be applied instead.

Power up values can be specified for digital and binary inputs (DI, BI) with location COM, digital and binary outputs (DO, BO), analog outputs (AO), markers (M), counters (C), and registers (R).

Fault reaction

Determines the fault reaction state of all IO points with exception of BO and hardware allocated BI.

Table 32 on page 399 shows the possible fault reaction settings for hardware IO.

Table 32 Fault Reaction settings for hardware IO

| Signal type | Fault Reaction settings |
|-----------------|----------------------------------|
| Digital Inputs | High/Low/Scan/Hold |
| Digital Outputs | Low/Appl |
| Analog Inputs | Top Scale/Bottom Scale/Scan/Hold |
| Analog Outputs | 0 mA/Appl |

Table 33 on page 399 shows the possible fault reaction settings for communication IO.

Table 33 Fault Reaction settings for communication IO

| Signal type | Fault Reaction settings |
|---|-------------------------|
| Digital Points (DI) | High/Low/Freeze |
| Numeric Points (BI) (The default fixed value for numerics is 0.) | Fixed Value/Freeze |

For more information, see *Overview Guide*.

Register type

The register type defines the format of the stored data. There are four different register types: Byte, Word, Long and Float. The first three (Byte, Word and Long) are integer values, the last (Float) is a real value consisting of an exponent and a mantissa.

Table 34 on page 400 shows the numeric types and ranges.

Table 34 Overview of available numeric types and ranges

| Numeric | Type | Minimum value | Maximum value |
|----------------|---------|----------------|----------------|
| Byte (8-bit) | Integer | –128 | +127 |
| Word (16-bit) | Integer | –32,768 | +32,767 |
| Long (32-bit) | Integer | –2,147,483,648 | +2,147,483,647 |
| Float (32-bit) | Real | -10^{38} | $+10^{38}$ |

Signal type

The signal type is used for analog inputs and outputs (AI and AO). It should match the used hardware configuration. The following signal types are available:

- 0 to 5 V
- 1 to 5 V
- 0 to 10 V
- 2 to 10 V
- 0 to 20 mA
- 4 to 20 mA,

Scaling

The signal type is used for analog inputs (AI). It assigns scaling properties to an analog point, allowing engineering units to be processed in the application. If this option is checked, then both **Bottom scale** and **Top scale** must be entered.

Bottom scale

The bottom scale of an analog point should contain a value in engineering units which is read or written on the bottom value of the defined signal type. If, for example, a temperature of 20°C is measured at a sensor voltage of 2 V (for a signal type of 2-10 V), you should enter 20 as the bottom scale value.

Top scale

The top scale of an analog point must contain a value in engineering units which is read or written on the top scale value of the defined signal type. If, for example, a temperature of 35°C is measured at a sensor voltage of 10 V (for a signal type of 2-10 V), you should enter 35 as the top scale value.

Transmitter alarm


The transmitter alarm fields low and high should contain a value in engineering units which is equal to or exceeds the values in **Bottom scale** and **Top scale**.

If a point value exceeds the boundaries set in transmitter alarm setting high and low, the value will be regarded as faulty.

Eng units (Engineering units)

The engineering units are used with analog inputs (AI), analog outputs (AO), and binary outputs (BO). The engineering units are defined as a string with a maximum length of five characters of the unit which is read or written with the point, for example °C, Psi, %.

Allocation attributes



Note:

When a point is used in an FLD but the point is not allocated, the application will not compile.

Allocation attribute fields must be filled if the point is to be used in the application.

Allocation can be done before, during, or after using a point in an FLD.

The following allocation attributes can be distinguished:

| Topic | See |
|--------------------------|----------|
| Size | page 402 |
| Chassis | page 403 |
| Slot | page 403 |
| Channel | page 403 |
| Communication allocation | page 403 |
| Field input device type | page 405 |

Size

In case of BIs and BOs this attribute defines the number of used allocated IO channels on an IO module for hardware allocated BIs and BOs. For example, a word can be divided bit-by-bit over 16 channels.

Once a size is chosen, a new choice can be made by first choosing **Chassis > Undefined** and then choosing a different **Size**.

If a size is chosen that needs a number of channels that doesn't fit on one module (taking into account the starting channel) a second module can be chosen to continue the allocation.

Safety Builder will automatically change the Register type to the smallest value able to contain the number of bits as defined by **Size**.

If, for example, a Binary point with Register type "Word" and Size "6" is allocated to hardware, only the first 6 bits of the Binary point are used to allocate. This means that the Register type is changed to "Byte".

Chassis

This attribute defines the chassis in which the point is allocated.

Once a chassis is chosen, a new choice can be made by first choosing **Chassis > Undefined**.

Slot

This attribute defines the slot in which the point is allocated. Before you designate a slot, you must first select a chassis.

Once a slot is chosen, a new choice can be made by first choosing **Chassis > Undefined** and then choosing a different **Chassis** and **Slot** value.

Channel

This attribute defines the channel in which the point is allocated. Before you designate a channel, you must first select a chassis and slot.

Once a channel is chosen, a new choice can be made by first choosing **Chassis > Undefined** and then choosing a different **Chassis**, **Slot** and **Channel** value.

Communication allocation

You can communicate the value of a point from/to an external device or an SM Controller by configuring the communication allocation settings for that point.

- You can receive values from external devices or other SM Controllers via input points in Safety Manager with the location COM (for values from external devices) or location FSC (for values from other SM Controllers). To allocate these input points you must assign a logical connection and a PLC address to the **Input** communication allocation field of that point, as shown in Figure 85 on page 404.
- You can send the value of *any* point to external devices or SM Controllers by configuring a logical connection and a PLC address to an **output** communication allocation field of that point.

Figure 85 Setting communication allocations on an input point with location COM

Communication allocation

| Type | Logical connection | PLC address |
|--------|-------------------------------|-------------|
| Input | Experion Server-SM Controller | 10001 |
| Output | Undefined | |

Undefined
Safety Builder-SM Controller_1
DCS-SM Controller_1
SM Controller_1-SM Controller_2
SM Controller_1-SM Controller_3



Note:

You can create multiple output communication allocations for one point by assigning (multiple) logical connections.

You do not need to create a dedicated output with location COM or FSC for each communicated point.

To send or receive a point by means of communication, you must:

- 1 assign a logical connection. (See “Assigning a logical connection” on page 404)
- 2 assign a PLC address. (See “PLC address” on page 405)

Assigning a logical connection



Note:

Before assigning a logical connection you must have logical connections configured in the Network Configurator.

The following parameters are relevant to assign a logical connection:

- **Type**
Choose between Input (data received - only valid for input points with location COM) and Output (data sent).
- **Logical connection**
Choose which available master-slave logical connection is to be used.
- **PLC address**
Choose which available PLC address is to be used.

**Tip:**

Figure 85 on page 404 shows an example of assigning a logical connection to an input point.

PLC address

The available PLC addresses for communication allocation of points depends on:

- type of communication channel
- type of point
- Reserved PLC addresses

Experion address ranges

- Points of type DI and DO can be assigned in the range of 1 to 8192.
- Points of type AI, BI, BO and AO can be assigned in the range of 10001 to 18192.

Safety Builder address ranges

- The Safety Builder marker PLC addresses range from 0 to 29999.
- The Safety Builder register PLC addresses range from 32000 to 65534.

DCS address ranges

- The Modbus marker PLC addresses range from 1 to 65535.
- The Modbus register PLC addresses range from 1 to 65535.
Long Words and Floats get 2 PLC addresses assigned. The most significant value in the sequence is stored at the lowest storage address.

CEE controller address ranges

- The CEE controller marker PLC addresses range from 1 to 65535.
- The CEE controller register PLC addresses range from 1 to 65535.
Long Words and Floats get 2 PLC addresses assigned. The most significant value in the sequence is stored at the lowest storage address.

Field input device type

Here you allocate the type of field input device for line monitored digital inputs.

Depending on the field input device the sensitivity, range and line monitoring settings of the allocated channel will be adapted.

The following field input devices can be selected:

- Namur sensors (SN);
- Namur sensors (SN) with Intrinsically Safe interface;
- Namur sensors (S1N);
- Namur sensors (S1N) with Intrinsically Safe interface;
- Fail Safe Namur (SN) sensors;
- Fail Safe Namur (SN) sensors with Intrinsically Safe interface
- Fail Safe Namur (S1N) sensors;
- Fail Safe Namur (S1N) sensors with Intrinsically Safe interface
- Digital switch with Loop monitoring;
- Digital switch without Loop monitoring;
- No input device

For details regarding these field input devices, see the *Hardware Reference*.

System attributes



Attention:

It is strongly recommended not to change system attributes manually if you are not sure what you are doing.

System attributes are attribute fields filled by an configuration tool, such as Application Editor.

If desired you can manually alter the system attributes in Point Configurator, although it is recommended to use the Application Editor for this purpose.

The following system attributes can be distinguished:

| Topic | See |
|---------------|----------|
| FLD number | page 407 |
| Timer base | page 407 |
| Timer value | page 408 |
| Counter range | page 408 |

FLD number

This is number of the Functional Logic Diagrams that contains the point. A point can only be used on one FLD. If you want to use the value of a point on more FLDs, you can use sheet transfers.

Timer base

This is the period in which the timer is counting down by one. This can be 100 milliseconds (100 ms), 1 second (1 s), or 1 minute (1 m). The timer base is the period in which the timer is counted down by one.



Note:

This value can only be set in the Application Editor.

Timer value

This is the multiplier value for the time base. Please note that this value is not necessarily the same as the value that you initially entered in the Application Editor. Depending on the timer value you entered in the FLD, the time base of the timer may be changed in order to optimize the timer resolution. For more information on timers, see “Time functions details” on page 375.

Counter range

This is the range that can be assigned to a counter.

The counter output becomes TRUE when the counter reaches the maximum counter value ($1 \leq \text{Max} \leq 8191$).

For more information see “Counter” on page 362.

Import and Export

E

APPENDIX

With the **Import Points** and **Export Points** functions in **Point Configurator** you import or export a point database containing the main attributes of all points in Safety Manager.

This appendix describes the configuration and formats applied for the external point database. It also describes the records of an exported database and the format and import/design rules for a database which is to be imported.

| Topic | See |
|--|----------|
| Database setup and field properties | page 410 |
| Database formats supported | page 416 |
| Creating and importing from an external database | page 423 |
| Log file | page 439 |

Database setup and field properties

This section addresses the usage and properties of the available fields (field records) of external point databases.

Database setup

Figure 86 on page 410 shows an example of an exported database.

- The first row is a heading row, containing the names of all field columns.
- All other rows contain point related information.
- Each column contains an actual field parameter that may, or may not, be used as point information:
 - some columns are mandatory,
 - some columns are optional; their use depends on settings in other columns.



Note:

1. Note that not all field columns will be used: e.g. digital input points will not use the timer related field columns, whereas timer points do.
2. Irrelevant field columns are usually left empty, contain a default (exported) value or are removed from a database before importing.

Figure 86 Example of an exported database open in Excel

| | | Fieldname | | | | | | | | |
|-------|----|-----------------------|--------------|-----------|----------|------|---------|---------------|----------------------------------|-----------------|
| | | A | B | C | D | E | F | G | H | I |
| Point | 1 | TagNumber | NewTagNumber | PointType | Location | Unit | SubUnit | Status | Description | Salary/Rate/etc |
| | 2 | C400_1_N | | M | | | | | Function block marker | Undefined |
| | 3 | C552_2_C | | M | | | | | Function block marker | Undefined |
| | 4 | 342_2 | | T | | | | | | Undefined |
| | 5 | 13PIT42J15/17/18HH_FF | | DO | COM | | | FAILED | PARTIAL FAILURE | No |
| | 6 | 13_42_C6S1_S2 | | DO | COM | | | NOT FAULTY | AI MODULE STATUS | No |
| | 7 | 13ZS0420046 | | DI | FLD | | | OPEN | PRODUCTION TO EXPORT LINE BYPASS | Yes |
| | 8 | 530_0 | | M | | | | | | Undefined |
| | 9 | 13LIT422008_HHINH | | DI | COM | | | INHIBIT | HH START UP INHIBIT FROM HMI | No |
| | 10 | 1060_1 | | T | | | | | | Undefined |
| | 11 | C670_3_D | | R | | | | | Function block register | Undefined |
| | 12 | 610_914_1 | | M | | | | NOT HIGH HIGH | 13PIT42A08 HH | Undefined |
| | 13 | 102_555_6 | | M | | | | INHIBIT | INHIBIT ALLOWED | Undefined |
| | 14 | C210_1_F | | M | | | | | Function block marker | Undefined |
| | 15 | 13SOV42C03A_PCS | | DI | COM | | | OPEN | OPEN INT FROM PCS | No |
| | 16 | 13PSD3_42D_1_RST | | DO | COM | | | RESET | RESET FEEDBACK TO HMI | No |
| | 17 | 1026_2 | | T | | | | | | Undefined |
| | 18 | 104_760_6 | | M | | | | INHIBIT | INHIBIT ALLOWED | Undefined |
| | 19 | 822_1262_1 | | M | | | | NOT HIGH HIGH | 13PIT420079 HH | Undefined |
| | 20 | 1266_11 | | M | | | | | | Undefined |
| | 21 | 13SOV42F01_VOPEN | | DO | COM | | | OPEN | SOV OPEN TO HMI | No |

Database field properties

This section discusses all field columns of external databases, as indicated in “Database setup” on page 410.

This section is divided in the following subsections:

- “The database field properties table explained” on page 411
- “Database field properties table” on page 412.

The database field properties table explained



Note:

For practical reasons the field columns of the actual database are presented as rows.

Whereas the columns in the actual database (as in Figure 86 on page 410) provide the *field records of each point*, the columns in Table 36 on page 412 provide the *properties of each field record*.

The available properties of each field record in Table 36 on page 412 are explained in Table 35 on page 411.

Table 35 Database field properties table explained

| Field name & field type [...] | option | Content / range | Example | Description / Remarks |
|-------------------------------|--------|-----------------|---------|-----------------------|
| * | ** | *** | **** | ***** |

- * Shows field name and field properties. The meaning of the field name is explained in the column “Description / Remarks”. For field properties such as field type and format see “Database formats supported” on page 416.
- ** Identifies that the field can be exported and if the field can be imported. Fields that cannot be imported must be removed before re-importing a database.
- *** Lists the type and format of the content of a field. Some fields use values, others use a string to record point specific settings. For more information see “Strings and field formats” on page 416.
- **** Provides an example of the content.
- ***** Provides a short description and reference to the type of field and contains additional remarks, if any.

Database field properties table

Table 36 on page 412 describes all fields that are available for points in the external database.

Table 36 Database field properties

| Field name & field type [...] | option | Content / range | Example | Description / Remarks |
|---|------------------|---|--------------------------------|---|
| <i>TagNumber</i> [text] | export import | text up to 32 characters | LT-1130-1 | Describes the tag number. For details, see “Tag number” on page 394. Obligatory information |
| <i>NewTagNumber</i> [text or string] | import | text up to 32 characters representing a command or tag number | DELETE or LT-2130-A | Contains a command or a new tag number for the related point. For details, see “Command fields” on page 417. |
| <i>PointType</i> * [string] | export import | See “PointType strings” on page 419 | AI | Describes the point type. For details, see “Point Type” on page 393. Obligatory information |
| <i>Location</i> [text or string] | export import | text up to 3 characters or a string; see “Location strings” on page 420 | FLD | Describes the point location. For details, see “Location” on page 394. If not identified as string, the data is treated as text. |
| <i>Unit</i> [text] | export import | text up to 8 characters | SHEET 1 | Describes the point unit location. For details, see “Unit” on page 395. |
| <i>SubUnit</i> [text] | export import | text up to 8 characters | LOGIC 40 | Describes the point subunit location. For details, see “Subunit” on page 395. |
| <i>Status</i> [text] | export import | text up to 16 characters | High temp | Describes the status of boolean point types. For details, see “Status” on page 394. |
| <i>Description</i> [text] | export import | text up to 64 characters | Temperatu re boiler 1130 | Provides a description of the point. For details, see “Point Type” on page 393. |
| <i>SafetyRelated</i> [string] | export import | See “SafetyRelated strings” on page 420 | Yes | Indicates the desired safety relation. For details, see “Safety related” on page 396. |

Table 36 Database field properties (continued)

| Field name & field type [...] | option | Content / range | Example | Description / Remarks |
|--------------------------------------|------------------|--|-----------|---|
| <i>Size</i> [numeric] | export import | Integer 1..31 | 12 | Indicates the desired size in case a binary point is allocated. For details, see “Size” on page 402. |
| <i>ChassisIDAsString</i> [string] | export import | See “ChassisIDAsString string” on page 422 | 01.02 | Identifies the IO Chassis the point is allocated on. For details, see “Chassis” on page 403. |
| <i>SlotNumber</i> [numeric] | export import | Integer 1..18 | 12 | Identifies the IO module slot the point is allocated on. For details, see “Slot” on page 403. |
| <i>ChannelNumber</i> [numeric] | export import | Integer 1..17 | 3 | Identifies the IO module channel the point is allocated on. For details, see “Channel” on page 403. |
| <i>ForceEnable</i> [boolean] | export import | FALSE; TRUE | TRUE | Provides the ability to force the point. For details, see “Force enable” on page 398. |
| <i>WriteEnable</i> [boolean] | export import | FALSE; TRUE | FALSE | Provides the ability to write the point. For details, see “Write enable” on page 399 |
| <i>PowerUpValue</i> [numeric] | export import | float or 0..1** | 0 | Provides the power up value for output points. For details, see “Power up” on page 399 |
| <i>SIL</i> [text] | export import | text up to 12 characters | SIL 2 | Indicates the SIL level of the point. For details, see “SIL” on page 395 |
| <i>FLDNumber</i> [numeric] | export | integer 1..2499 | 200 | Provides the FLD number the point is used on. For details, see “FLD number” on page 407 |
| <i>RegisterType</i> [string] | export import | See “RegisterType strings” on page 420 | Undefined | Provides the type of register for register points. For details, see “Register type” on page 400 |
| <i>SignalType</i> [string] | export import | See “SignalType strings” on page 420 | 4–20mA | Provides the type of field signal for analog input points. For details, see “Signal type” on page 400 |
| <i>Scaling</i> [boolean] | export import | FALSE; TRUE | TRUE | Allows processing of analog points in engineering units. For details, see “Scaling” on page 400 |
| <i>BottomScale</i> [numeric] | export import | float | 0 | Provides the bottom scale for an analog point. For details, see “Bottom scale” on page 400 |

Table 36 Database field properties (continued)

| Field name & field type [...] | option | Content / range | Example | Description / Remarks |
|--|------------------|--|--------------------|--|
| <i>TopScale</i> [numeric] | export import | float | 100 | Provides the topscale for an analog point. For details, see “Top scale” on page 401 |
| <i>EngineeringUnits</i> [text] | export import | text up to 8 characters | Celsius | Provides the engineering units for scaled analog points. For details, see “Eng units (Engineering units)” on page 401 |
| <i>TimerBase</i> [string] | export import | See “TimerBase strings” on page 420 | Undefined | Provides the timer base for timer points. For details, see “Timer base” on page 407 |
| <i>TimerValue</i> [integer] | export import | integer 0..2 ²³ | 0 | Provides the timer value for timer points. For details, see “Timer value” on page 408 |
| <i>Range</i> [numeric] | export import | integer 0..32767 | 0 | Provides the counter range for counter points. For details, see “Counter range” on page 408 |
| <i>ApplicationAddress</i> [numeric] | export | integer 0..32767 | Invalid | Provides the internal application address for points. |
| <i>FaultReaction</i> [string] | export import | See “FaultReaction string” on page 420 | Undefined | Provides the fault reaction state of the point. For details, see the <i>Safety Manual</i> . |
| <i>FaultReactionValue</i> [numeric] | export import | float | 0 | Provides the preset value for BI points. For details, see the <i>Safety Manual</i> . |
| <i>FieldInputDevice</i> [string] | export import | See “FieldInputDevice string” on page 421. | Namur sensors (SN) | Provides the field device properties for line monitored DI points. |
| <i>SOESetPointLow</i> [numeric] | export import | float | 0 | Provides the lower and higher SOE set points for analog points. |
| <i>SOESetPointHigh</i> [numeric] | export import | float | 0 | |
| <i>SOEID</i> [numeric] | export | integer 0..65535 | 548 | Provides the SOE sequence number for SOE enabled points. |
| <i>TransmitterAlarmLow</i> [numeric] | export import | float | 0 | Provides the lower and higher alarm set points for analog input points. For details, see “Transmitter alarm” on page 401 |
| <i>TransmitterAlarmHigh</i> [numeric] | export import | float | 3428 | |

Table 36 Database field properties (continued)

| Field name & field type [...] | option | Content / range | Example | Description / Remarks |
|---------------------------------------|------------------|---|------------------------|---|
| <i>TimerType</i> [string] | export import | See “TimerType strings” on page 421 | Undefined | Provides the type of timer for timer points. For details, see “Timers” on page 371. |
| <i>ComAllocationType#</i> [string] | export import | See “ComAllocation Type# string” on page 422 | Output | Provides additional communication allocation details for this point. For details about communication allocation see “Communication allocation” on page 403. |
| <i>Master#</i> [string] | export import | See “Master# and Slave# strings” on page 422. | name of logical Master | Note: “#” represents a decimal number allowing for duplication of that field. For more information on duplicate fields, see “Duplicate fields” on page 418. |
| <i>Slave#</i> [string] | export import | | name of logical Slave | |
| <i>PLCAddress#</i> [numeric] | export import | integer 0..65535 *** or empty | 25 | |

* You cannot *create* new points of type M, C, T and R by importing these into the database.

** For digital outputs you can only use 0 (indicates a low) or 1 (indicates a high) as power up value.

*** You must leave *PLCAddress#* empty when allocating from/to another SM Controller. For details see “Points of attention when importing a database” on page 424.

Database formats supported

This section provides information regarding the file types and field formats used for external point databases.

File types supported

The following file types are supported with the current version of Safety Builder:

- Microsoft Excel *.xls file types.

Strings and field formats

The external point database exists of fields containing data of a certain kind and format. These fields are available for each point and together they determine the point's main settings.

This section details the various types and formats that are supported. For information on field *usage*, see “Database setup and field properties” on page 410.

The following data types and formats are supported:

- “Field formats” on page 416
- “Command fields” on page 417
- “Duplicate fields” on page 418
- “String fields” on page 419

Field formats

The following field types are supported:

- “Boolean” on page 416
- “Numeric” on page 417
- “Text” on page 417

Boolean

Boolean fields are formatted to contain either the value `FALSE` or `TRUE`.

A boolean field can be formatted as a boolean field but it can also be formatted as a text field (for details, see “Text” on page 417). When formatted as text field it may *only* contain the strings `FALSE` or `TRUE`.

Numeric

Numeric fields are formatted to contain numerical values.

The type of numeric is indicated by the *RegisterType* field. The numeric type set by this field also determines the maximum range of that numeric.

- **Integer**

This is a numeric containing whole values (with increments of 1).

Integers have limited value ranges and are defined by the *RegisterType* setting Byte, Word or Long.

- **Float**

This is a numeric containing decimal values (approaching real numbers with increments close to 0).

Floats have a range of -1E38 to +1E38 and are defined by the *RegisterType* setting Float.

Text

Text fields are formatted to contain alphanumeric characters. Whatever they contain is treated as text.

Text fields have a limited number of characters they can contain. For details see “Database setup and field properties” on page 410.

Command fields

Command fields are fields containing text that is interpreted as a command towards to the related point.

Command fields must be empty or contain a valid text command when read by Safety Builder upon import.

- Command fields are empty upon export.
- Empty command fields are ignored (no command) during import.

The following command text is recognized:

- **DELETE** (any combination of upper and lower case characters allowed);
When this text is found in a command field during import the related tag number is deleted from the point database.
- up to 32 characters representing a new tag number;
When a set of characters is detected during import, that is not recognized as a command, it is regarded as a new tag number: the current tag number is renamed to the new tag number.

For details about tag number naming, see “Tag number” on page 394.

Duplicate fields

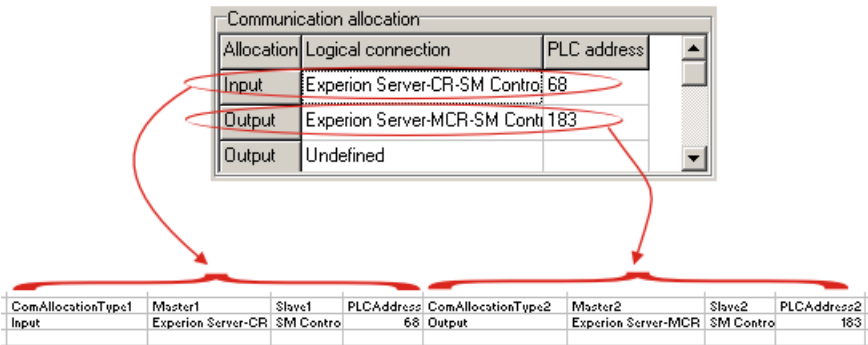
Duplicate fields are fields that can be re-used several times for a single point.

- Duplicate fields are fields that have a decimal extension represented by the number sign “#”.
By making the extension number unique, a field can be assigned multiple times (see Example on page 418)
- To duplicate a field you must copy it and renumber its decimal extension.

Example

Suppose you want to allocate a *single* point on *multiple* external communication devices / SM Controllers as shown in Figure 87 on page 418.

Figure 87 Allocate a single point on multiple communication devices using duplicated fields



To realize this you use duplicated communication allocations for a single point.

Tips:

1. See “Communication allocation” on page 403 for more information about this topic.
2. See “String fields” on page 419 for more information about the communication allocation strings.

- 1 Create the *first* communication allocation group by creating the following columns:
 - *ComAllocationType1;Master1;Slave1;PLCAddress1*
- 2 Create the *second* communication allocation group by creating these columns:
 - *ComAllocationType2;Master2;Slave2;PLCAddress2*
- 3 Fill the columns with appropriate data.

Rules when duplicating

Note that the following rules apply when you duplicate fields:

- You may only number as high as the maximum allowable number of fields. E.g. if you have 3 logical connections in an SM Controller you may choose any number between 1, 2 and 3 to identify a group of duplicated communication allocation fields.
- A set of duplicated fields belong together if they:
 - have the same number and
 - belong to the same group.
- When importing communication allocation groups, the *relation Master#-Slave#* determines to which communication allocation group is referred, *not the column order or the decimal extension*.

String fields

String fields are text formatted field types (as described in “Text” on page 417) containing a set of *predefined* alphanumeric characters.

A string is a set of predefined alphanumeric characters used to identify certain point settings such as *SafetyRelated*, *PointType*, *RegisterType*, etc.



Attention:

When creating a database all imported strings must be entered as indicated in the sections below. Capitalization is ignored, but all other aspects of a string must be *exactly* as indicated.

If a string is not entered correctly it cannot be recognized by Safety Builder and will cause the import action to cancel.



Tip:

To make sure you enter the string correctly you can copy a string value from an exported database.

Below headings list the supported string types in chronological order.

PointType strings

The following strings can be used to identify the point type:

```
DI; AI; BI;
DO; AO; BO;
M; C; T; R
```

For information about these strings see “Point Type” on page 393.

Location strings

For points where the *Location* field is mandatory the following strings can be used to identify predefined point locations:

SYS; FSC; COM

For information about these strings see “Location” on page 394.

SafetyRelated strings

For points where the *SafetyRelated* field is valid the following strings can be filled to identify the point safety settings:

No; Yes

For information about these strings see “Safety related” on page 396.

RegisterType strings

For points where the *RegisterType* field is valid the following strings can be filled to identify the register type:

Word; Byte; Long; Float

For information about these strings see “Register type” on page 400.

SignalType strings

For points where the *SignalType* field is valid the following strings can be used to identify the point signal type:

0-5V; 1-5V;

0-10V; 2-10V;

0-20mA; 4-20mA

For information about these strings see “Signal type” on page 400.

TimerBase strings

For points where the *TimerBase* field is valid the following strings can be used to identify the point’s base timer:

10 ms; 100 ms;

1 s; 1 min

FaultReaction string

For points where the *FaultReaction* field is valid the following strings can be used to identify the point fault reaction settings:

High; Low; Scan

Freeze; Fixed Value

For information about these strings see the *Safety Manual*.

FieldInputDevice string

For points where the *FieldInputDevice* field is valid the following strings can be used to identify the field input device connected to a point:

```
Namur sensors (SN);
Namur sensors (SN) with Intrinsically Safe interface;
Namur sensors (S1N);
Namur sensors (S1N) with Intrinsically Safe interface;
Fail Safe Namur (SN) sensors;
Fail Safe Namur (SN) sensors with Intrinsically Safe
interface
Fail Safe Namur (S1N) sensors;
Fail Safe Namur (S1N) sensors with Intrinsically Safe
interface
Digital switch with Loop monitoring;
Digital switch without Loop monitoring;
No input device
```

For information about these strings see “Field input device type” on page 405.

TimerType strings

For points where the *TimerType* field is valid the following strings can be used to identify the type of timer configured:

```
Pulse with constant timer value;
Pulse retriggerable with constant timer value;
Delayed ON with constant timer value;
Delayed ON memorize with constant timer value;
Delayed OFF with constant timer value;
Pulse with variable timer value;
Pulse retriggerable with variable timer value;
Delayed ON with variable timer value;
Delayed ON memorize with variable timer value;
Delayed OFF with variable timer value
```

For information about these strings see “Timers” on page 371.

ChassisIDAsString string

For points that are allocated to field IO, the *ChassisIDAsString* field must be filled. This string can be used to identify the IO chassis the point is allocated on.

This string consists of two 2-digit string values, separated by a dot:

`"controllernodeno.chassis"`



Note:

"controllernodeno" and "chassis" should be replaced by 2-digit string values, as identified in **Network Configurator**, **Hardware Configurator** or the exported database.

For information about this string see "Chassis" on page 403.

ComAllocationType# string

For points where the *ComAllocationType#* field is valid the following strings can be used to identify the type of communication allocation:

`Input; Output`



Note:

ComAllocationType# is a duplicate string field.
For details about duplicate fields see "Duplicate fields" on page 418.

For information about these strings see "Communication allocation" on page 403.

Master# and Slave# strings

For points where the *ComAllocationType* field is valid the following strings can be used to identify the communication master and the communication slave of the communication allocation:

`"name of logical device"`



Note:

1. "name of logical device" should be replaced by the actual string identifying the communication device or SM Controller configured in the **Logical View** of **Network Configurator** or an exported database.
 2. Master# and Slave# are duplicate string fields.
For details about duplicate fields see "Duplicate fields" on page 418.
-

For information about these strings see "Communication allocation" on page 403.

Creating and importing from an external database

This section describes the methods for and limitations of creating external databases.

Quick reference for importing a database

**Tip:**

The performance of the Import function is related to the database size; by decreasing the database size you increase the performance of the import function!

You can quickly create and import a valid external database by performing the following steps:

- 1 Export an existing (empty) point database from Safety Builder.
- 2 *Optional:* Select and delete all columns that do not need to be re-imported. **DO NOT** delete the *Tagnumber*, and *PointType* columns!
- 3 *Optional:* Reshuffle columns, if desired.
- 4 Insert as many new rows as new points are required.
- 5 *Optional:* Delete the rows with points that should not be modified.
- 6 Fill the table with the appropriate field values (see “Points of attention when importing a database” on page 424 and “Field record handling for database import” on page 425 for details).
- 7 Save and import the database.

Limitations of import function

When allocating, creating or modifying points via the import function you *cannot*:

1. create new logical symbols such as markers, timers, counters etc.
2. allocate binary signals on multiple IO modules
3. modify fields that are not user configurable via the Point Configurator.

Points of attention when importing a database



Note:

If a fault is detected during import, *no points will be imported*. The Import function is cancelled and an error log is generated. For details see “Log file” on page 439.

When importing an external database you should note the following:

- 1 The structure of the imported database must be identical to an exported database, with the exception that field columns may be omitted or reshuffled. For details see “Database formats supported” on page 416.
- 2 Obligatory field columns such as *Tagnumber* and *PointType* must always be present and valid, as the value of these records determine the interpretation of the other attributes (see below).
- 3 If the combination of *Tagnumber* and *PointType* identifies an existing point, the imported point attributes overwrite the existing point attributes. If the combination of *Tagnumber* and *PointType* does *not* identify an existing point, a new point is created containing all the imported point attributes.
- 4 Not imported attributes get their default value.
- 5 If the *Location* field column is not found, a default or empty Location is assumed. *This impacts the interpretation of other fields* as explained in “Field record handling for database import” on page 425.
- 6 The data in a field record is only imported if:
 - a. the data conforms the description in “Database setup and field properties” on page 410.
 - b. the data does not conflict with the point specific field handling rules as described in “Field record handling for database import” on page 425.
 - c. no errors occurred during the import session of the database.
- 7 If a single point is imported multiple times during an import session, the latest import action will be applied.
- 8 Do not state a value in the *PLCAddress#* field when creating a communication allocation between SM Controllers (i.e. SafeNet). Addresses to communicate point values between SM Controllers are defined automatically by Safety Builder.

Field record handling for database import

This section lists which field values can be imported in which field records and under what conditions.

This is done by means of tables, containing the properties and rules that apply to each field record.

The following subsections list the available field record tables:

- “Field record handling related to digital inputs” on page 426
- “Field record handling related to digital outputs” on page 428
- “Field record handling related to binary inputs” on page 430
- “Field record handling related to binary outputs” on page 432
- “Field record handling related to analog in- and outputs” on page 434
- “Field record handling related to logical symbols” on page 436

Available field record tables



Note:

The following applies to field interpretation Table 37 on page 426 through field interpretation Table 42 on page 437:

1. The default values in the column **Fieldname** only apply for new imported points. If an imported point should already exist, the existing value becomes its default.
2. The text between square brackets [...] indicates the *Location* types that can be defined for a point.
Each column **point_X [Location_Y]** lists the available choices and/or actions for that type of point and location.
3. **Import value** can only be executed when the copied field value is valid, i.e. of the right type and size. Else a fault is reported and the *entire* import action is cancelled.
4. To get a list of valid field values, types and sizes, see “Database formats supported” on page 416 and “Database setup and field properties” on page 410.

Field record value codes

The listed field record values in above mentioned subsections consist of below mentioned properties.

| | |
|---------------------|---|
| text | means that you should enter text |
| string | means that you should enter a string value (predefined text) |
| “STRING1, STRING 2” | means that the choice in string values is limited to the listed options |
| boolean | means that you should enter a boolean value |

| | |
|------------|--|
| numeric | means that you should enter a numeric value |
| default | means that you should not change the field value |
| ..or empty | by blanking this field no value is imported |

Field record handling related to digital inputs

Table 37 on page 426 shows the data expected for imported field records related to digital inputs.

For more information on the type of data that is expected in a record, see “Database setup and field properties” on page 410.


| | |
|---|--|
|  | <p>Note:</p> <ol style="list-style-type: none">1. For a good understanding of this table you should first read “Creating and importing from an external database” on page 423.2. As the validity of a field record depends on the value in the Location field <i>and</i> on the type of point, you see one column with values per location type. |
|---|--|

Table 37 Valid field values when importing digital inputs

| Field name & default value | DI [COM] | DI [FSC] | DI [SYS] | DI [other] |
|---|--------------------------|--------------------------|-------------------------------------|--------------------------|
| <i>NewTagName</i> default = empty | empty or command text | empty or command text | empty or command text | empty or command text |
| <i>Unit</i> default = no text | text | text | text | text |
| <i>SubUnit</i> default = no text | text | text | text [*] | text |
| <i>Status</i> default = no text | text | text | text ^{**} | text |
| <i>Description</i> default = no text | text | text | text ^{***} | text |
| <i>SafetyRelated</i> default = No | default or empty | string or empty | default or empty ^{****} | string or empty |
| <i>Size</i> default = empty | default or empty | default or empty | default or empty | numeric or empty |
| <i>ChassisIDAsString</i> default = empty | default or empty | default or empty | default or empty | string or empty |
| <i>SlotNumber</i> default = empty | default or empty | default or empty | default or empty | numeric or empty |
| <i>ChannelNumber</i> default = empty | default or empty | default or empty | default or empty | numeric or empty |

Table 37 Valid field values when importing digital inputs (continued)

| Field name & default value | DI [COM] | DI [FSC] | DI [SYS] | DI [other] |
|--|-------------------------------------|-------------------------------------|----------------------|----------------------|
| <i>ForceEnable</i> default = False | boolean or empty | boolean or empty | default or empty | boolean or empty |
| <i>WriteEnable</i> default = False | boolean or empty | default or empty | boolean or empty | default or empty |
| <i>PowerUpValue</i> default = 0 | 0, 1 or empty | 0, 1 or empty | default or empty | default or empty |
| <i>SIL</i> default = no text | text or empty | text or empty | text or empty | text or empty |
| <i>RegisterType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SignalType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Scaling</i> | default or empty | default or empty | default or empty | default or empty |
| <i>BottomScale</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TopScale</i> | default or empty | default or empty | default or empty | default or empty |
| <i>EngineeringUnits</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerBase</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerValue</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Range</i> | default or empty | default or empty | default or empty | default or empty |
| <i>FaultReaction</i> default = Low | “Low, High, Freeze”, or empty | “Low, High, Freeze”, or empty | default or empty | default or empty |
| <i>FaultReactionValue</i> | default or empty | default or empty | default or empty | default or empty |
| <i>FieldInputDevice</i> default = Undefined | default or empty | default or empty | default or empty | string or empty |
| <i>SOESetPointLow</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SOESetPointHigh</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmLow</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmHigh</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ComAllocationType#</i> default = empty | string or empty | string or empty | “Output” or empty | “Output” or empty |
| <i>Master#</i> default = empty | string or empty | string or empty | string or empty | string or empty |
| <i>Slave#</i> default = empty | string or empty | string or empty | string or empty | string or empty |
| <i>PLCAddress#</i> default = empty | numeric or empty | default or empty | numeric or empty | numeric or empty |

- * SubUnit is empty, except where the *DI [SYS]* point has the tag name `InputLoopFault`. In that case the SubUnit value is a text.
- ** Status value is empty if *DI [SYS]* concerns a flasher point.
- *** Each *DI [SYS]* point type has its own default description.
- **** All *DI [SYS]* point types are safety related (`Yes`), except for flasher points.

Field record handling related to digital outputs

Table 38 on page 428 shows the handling of imported field records related to digital outputs.

For more information on the type of data that is expected in a record, see “Database setup and field properties” on page 410.



Note:

1. For a good understanding of this table you should first read “Creating and importing from an external database” on page 423.
2. As the validity of a field record depends on the value in the `Location` field *and* on the type of point, you see one column with values per location type.

Table 38 Database field interpretation for digital outputs

| Field name & default value | DO [COM] | DO [FSC] | DO [SYS] | DO [other] |
|---|--------------------------|--------------------------|--------------------------|--------------------------|
| <i>NewTagName</i> default = empty | empty or command text | empty or command text | empty or command text | empty or command text |
| <i>Unit</i> default = no text | text | text | text | text |
| <i>SubUnit</i> default = no text | text | text | text | text |
| <i>Status</i> default = no text | text | text | text | text |
| <i>Description</i> default = no text | text | text | text* | text |
| <i>SafetyRelated</i> default = No | default or empty | string or empty | default** or empty | string or empty |
| <i>Size</i> default = empty | default or empty | default or empty | default or empty | numeric or empty |
| <i>ChassisIDAsString</i> default = empty | default or empty | default or empty | default or empty | string or empty |
| <i>SlotNumber</i> default = empty | default or empty | default or empty | default or empty | numeric or empty |

Table 38 Database field interpretation for digital outputs (*continued*)

| Field name & default value | DO [COM] | DO [FSC] | DO [SYS] | DO [other] |
|--|------------------------|-------------------------|----------------------|-----------------------|
| <i>ChannelNumber</i> default = empty | default or empty | default or empty | default or empty | numeric or empty |
| <i>ForceEnable</i> default = False | boolean or empty | default or empty | default or empty | boolean or empty |
| <i>WriteEnable</i> default = False | boolean or empty | default or empty | default or empty | default or empty |
| <i>PowerUpValue</i> default = 0 | 0, 1 or empty | 0, 1 or empty | default or empty | 0, 1 or empty |
| <i>SIL</i> default = no text | text or empty | text or empty | text or empty | text or empty |
| <i>RegisterType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SignalType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Scaling</i> | default or empty | default or empty | default or empty | default or empty |
| <i>BottomScale</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TopScale</i> | default or empty | default or empty | default or empty | default or empty |
| <i>EngineeringUnits</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerBase</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerValue</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Range</i> | default or empty | default or empty | default or empty | default or empty |
| <i>FaultReaction</i> default = Low | default or empty | default or empty | default or empty | Low, Scan or empty |
| <i>FaultReactionValue</i> | default or empty | default or empty | default or empty | default or empty |
| <i>FieldInputDevice</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SOESetPointLow</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SOESetPointHigh</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmLow</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmHigh</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ComAllocationType#</i> default = empty | “Output” or empty | “Output” or empty | “Output” or empty | “Output” or empty |
| <i>Master#</i> default = empty | string or empty | string or empty | string or empty | string or empty |
| <i>Slave#</i> default = empty | string or empty | string or empty | string or empty | string or empty |
| <i>PLCAddress#</i> default = empty | numeric or empty*** | numeric or empty**** | numeric or empty | numeric or empty |

- * Each *DO [SYS]* point type has its own default description.
- ** The default *SafetyRelated* value for *DO [SYS]* is *Yes*.
- *** Leave *PLCAddress#* empty when allocating from/to another SM Controller. For details see “Points of attention when importing a database” on page 424.
- **** Leave *PLCAddress#* empty when allocating from/to another SM Controller. For details see “Points of attention when importing a database” on page 424.

Field record handling related to binary inputs

Table 39 on page 430 shows the handling of imported field records related to binary inputs.

For more information on the type of data that is expected in a record, see “Database setup and field properties” on page 410.



Note:

1. For a good understanding of this table you should first read “Creating and importing from an external database” on page 423.
2. As the validity of a field record depends on the value in the *Location* field *and* on the type of point, you see one column with values per location type.

Table 39 Database field interpretation for binary inputs

| Field name & default value | BI [COM] | BI [FSC] | BI [SYS] | BI [other] |
|---|--------------------------|--------------------------|----------------------|--------------------------|
| <i>NewTagName</i> default = empty | empty or command text | empty or command text | empty | empty or command text |
| <i>Unit</i> default = no text | text | text | text | text |
| <i>SubUnit</i> default = no text | text | text | text | text |
| <i>Status</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Description</i> default = no text | text | text | text | text |
| <i>SafetyRelated</i> default = No | default or empty | default or empty | default* or empty | string or empty |
| <i>Size</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ChassisIDAsString</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SlotNumber</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ChannelNumber</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ForceEnable</i> default = False | boolean or empty | boolean or empty | default or empty | boolean or empty |

Table 39 Database field interpretation for binary inputs (*continued*)


| Field name & default value | BI [COM] | BI [FSC] | BI [SYS] | BI [other] |
|--|--------------------------------------|--------------------------------------|--------------------------|--|
| <i>WriteEnable</i> default = False | boolean or empty | default or empty | default or empty | default or empty |
| <i>PowerUpValue</i> default = 0 | numeric or empty | numeric or empty | default or empty | default or empty |
| <i>SIL</i> default = no text | text or empty | text or empty | text or empty | text or empty |
| <i>RegisterType</i> default = Word | string or empty | string or empty | “Byte, Word” or empty | string** or empty |
| <i>SignalType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Scaling</i> | default or empty | default or empty | default or empty | default or empty |
| <i>BottomScale</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TopScale</i> | default or empty | default or empty | default or empty | default or empty |
| <i>EngineeringUnits</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerBase</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerValue</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Range</i> | default or empty | default or empty | default or empty | default or empty |
| <i>FaultReaction</i> default = Fixed Value | “Fixed Value, Freeze” or empty | “Fixed Value, Freeze” or empty | default or empty | “Fixed Value, Freeze***,” or empty |
| <i>FaultReactionValue</i> default = 0 | numeric or empty | numeric or empty | default or empty | numeric or empty |
| <i>FieldInputDevice</i> default = Undefined | default or empty | default or empty | default or empty | string or empty |
| <i>SOESetPointLow</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SOESetPointHigh</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmLow</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmHigh</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ComAllocationType#</i> default = empty | string or empty | string or empty | “Output” or empty | “Output” or empty |
| <i>Master#</i> default = empty | string or empty | string or empty | string or empty | string or empty |
| <i>Slave#</i> default = empty | string or empty | string or empty | string or empty | string or empty |
| <i>PLCAddress#</i> default = empty | numeric**** or empty | numeric***** or empty | numeric or empty | numeric or empty |

- * All *BI [SYS]* point types related to clock and date settings are *not* safety related (*No*). All other *BI [SYS]* point types, such as **RepairTimer**, are safety related (*Yes*).
- ** For *BI [other]* points the register type *Float* is not valid.
- *** For *BI [other]* points the default value is *Undefined*
- **** Leave *PLCAddress#* empty when allocating from/to another SM Controller. For details see “Points of attention when importing a database” on page 424.
- ***** Leave *PLCAddress#* empty when allocating from/to another SM Controller. For details see “Points of attention when importing a database” on page 424.

Field record handling related to binary outputs

Table 40 on page 432 shows the handling of imported field records related to binary outputs.

For more information on the type of data that is expected in a record, see “Database setup and field properties” on page 410.



Note:

1. For a good understanding of this table you should first read “Creating and importing from an external database” on page 423.
2. As the validity of a field record depends on the value in the *Location* field *and* on the type of point, you see one column with values per location type.

Table 40 Database field interpretation for binary outputs

| Field name & default value | BO [COM] | BO [FSC] | BO [other] |
|---|--------------------------|--------------------------|--------------------------|
| <i>NewTagName</i> default = empty | empty or command text | empty or command text | empty or command text |
| <i>Unit</i> default = no text | text | text | text |
| <i>SubUnit</i> default = no text | text | text | text |
| <i>Status</i> default = no text | text | text | text |
| <i>Description</i> default = no text | text | text | text |
| <i>SafetyRelated</i> default = No | default or empty | boolean or empty | boolean or empty |
| <i>Size</i> default = empty | default or empty | default or empty | numeric or empty |
| <i>ChassisIDAsString</i> default = empty | default or empty | default or empty | string or empty |

Table 40 Database field interpretation for binary outputs (*continued*)

| Field name & default value | BO [COM] | BO [FSC] | BO [other] |
|--|----------------------|----------------------|--------------------------------|
| <i>SlotNumber</i> default = empty | default or empty | default or empty | numeric or empty |
| <i>ChannelNumber</i> default = empty | default or empty | default or empty | numeric or empty |
| <i>ForceEnable</i> default = False | boolean or empty | default or empty | boolean or empty |
| <i>WriteEnable</i> | default or empty | default or empty | default or empty |
| <i>PowerUpValue</i> default = 0 | numeric or empty | numeric or empty | numeric* or empty |
| <i>SIL</i> default =no text | text or empty | text or empty | text or empty |
| <i>RegisterType</i> default = Word | string or empty | string or empty | “Byte, Word, Long” or empty |
| <i>SignalType</i> | default or empty | default or empty | default or empty |
| <i>Scaling</i> | default or empty | default or empty | default or empty |
| <i>BottomScale</i> | default or empty | default or empty | default or empty |
| <i>TopScale</i> | default or empty | default or empty | default or empty |
| <i>EngineeringUnits</i> | default or empty | default or empty | default or empty |
| <i>TimerBase</i> | default or empty | default or empty | default or empty |
| <i>TimerValue</i> | default or empty | default or empty | default or empty |
| <i>Range</i> | default or empty | default or empty | default or empty |
| <i>FaultReaction</i> | default or empty | default or empty | default or empty |
| <i>FaultReactionValue</i> | default or empty | default or empty | default or empty |
| <i>FieldInputDevice</i> | default or empty | default or empty | default or empty |
| <i>SOESetPointLow</i> | default or empty | default or empty | default or empty |
| <i>SOESetPointHigh</i> | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmLow</i> | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmHigh</i> | default or empty | default or empty | default or empty |
| <i>TimerType</i> | default or empty | default or empty | default or empty |
| <i>ComAllocationType#</i> default = empty | “Output” or empty | “Output” or empty | “Output” or empty |
| <i>Master#</i> default = empty | string or empty | string or empty | string or empty |
| <i>Slave#</i> default = empty | string or empty | string or empty | string or empty |

Table 40 Database field interpretation for binary outputs (*continued*)

| Field name & default value | BO [COM] | BO [FSC] | BO [other] |
|---------------------------------------|-----------------------------------|------------------------------------|---------------------|
| <i>PLCAddress#</i> default = empty | numeric or empty ^{**} | numeric or empty ^{***} | numeric or empty |

* *PowerupValue* for *BO [other]* must be an integer or long integer, it cannot be a float.

** Leave *PLCAddress#* empty when allocating from/to another SM Controller. For details see “Points of attention when importing a database” on page 424.

*** Leave *PLCAddress#* empty when allocating from/to another SM Controller. For details see “Points of attention when importing a database” on page 424.

Field record handling related to analog in- and outputs

Table 41 on page 434 shows the handling of imported field records related to analog in- and outputs.

For more information on the type of data that is expected in a record, see “Database setup and field properties” on page 410.



Note:

1. For a good understanding of this table you should first read “Creating and importing from an external database” on page 423.
2. As the validity of a field record depends on the value in the *Location* field *and* on the type of point, you see one column with values per location type.

Table 41 Database field interpretation for analog inputs and outputs

| Field name & default value | AI [SYS] | AI [other] | AO [any] |
|---|------------------|--------------------------|--------------------------|
| <i>NewTagName</i> default = empty | empty | empty or command text | empty or command text |
| <i>Unit</i> default = no text | text | text | text |
| <i>SubUnit</i> default = no text | text | text | text |
| <i>Status</i> | default or empty | default or empty | default or empty |
| <i>Description</i> default = no text | text | text | text |
| <i>SafetyRelated</i> default = No | default or empty | string or empty | string or empty |
| <i>Size</i> default = empty | default or empty | numeric or empty | numeric or empty |

Table 41 Database field interpretation for analog inputs and outputs (*continued*)

| Field name & default value | AI [SYS] | AI [other] | AO [any] |
|---|---------------------|---------------------|---------------------|
| <i>ChassisIDAsString</i> default = empty | default or empty | string or empty | string or empty |
| <i>SlotNumber</i> default = empty | default or empty | numeric or empty | numeric or empty |
| <i>ChannelNumber</i> default = empty | default or empty | numeric or empty | numeric or empty |
| <i>ForceEnable</i> default = False | default or empty | boolean or empty | boolean or empty |
| <i>WriteEnable</i> | default or empty | default or empty | default or empty |
| <i>PowerUpValue</i> default = 0 | default or empty | default or empty | numeric or empty |
| <i>SIL</i> default = no text | text or empty | text or empty | text or empty |
| <i>RegisterType</i> | default or empty | default or empty | default or empty |
| <i>SignalType</i> default = 4-20mA | default or empty | string or empty | string or empty |
| <i>Scaling</i> default = True | boolean or empty | boolean or empty | default or empty |
| <i>BottomScale</i> default = 0* | numeric or empty | numeric or empty | numeric or empty |
| <i>TopScale</i> default = 0** | numeric or empty | numeric or empty | numeric or empty |
| <i>EngineeringUnits</i> default = empty | string or empty | string or empty | string or empty |
| <i>TimerBase</i> | default or empty | default or empty | default or empty |
| <i>TimerValue</i> | default or empty | default or empty | default or empty |
| <i>Range</i> | default or empty | default or empty | default or empty |
| <i>FaultReaction</i> | default or empty | default or empty | default or empty |
| <i>FaultReactionValue</i> | default or empty | default or empty | default or empty |
| <i>FieldInputDevice</i> | default or empty | default or empty | default or empty |
| <i>SOESetPointLow</i> default = see note *** | numeric or empty | numeric or empty | numeric or empty |
| <i>SOESetPointHigh</i> default = see note **** | numeric or empty | numeric or empty | numeric or empty |
| <i>TransmitterAlarmLow</i> default, see note ***** | numeric or empty | numeric or empty | numeric or empty |

Table 41 Database field interpretation for analog inputs and outputs (*continued*)

| Field name & default value | AI [SYS] | AI [other] | AO [any] |
|---|----------------------|----------------------|----------------------|
| <i>TransmitterAlarmHigh</i> default, see note ***** | numeric or empty | numeric or empty | numeric or empty |
| <i>TimerType</i> | default or empty | default or empty | default or empty |
| <i>ComAllocationType#</i> default = empty | “Output” or empty | “Output” or empty | “Output” or empty |
| <i>Master#</i> default = empty | string or empty | string or empty | string or empty |
| <i>Slave#</i> default = empty | string or empty | string or empty | string or empty |
| <i>PLCAddress#</i> default = empty | numeric or empty | numeric or empty | numeric or empty |

* The BottomScale field is ignored if *Scaling* = False

** The TopScale field is ignored if *Scaling* = False

*** Identical to *TransmitterAlarmLow* (see note below)

**** Identical to *TransmitterAlarmHigh* (see note below)

***** If **Scaling** is False the default value for *TransmitterAlarmLow* = 491 (1967 for AI [SYS] points)

If **Scaling** is True the default value for *TransmitterAlarmLow* depends on the chosen SignalType: For 0-5V and 1-5V the default is 0.75 (2.5 for AI [SYS] points); for 0-10V and 2-10V the default is 2; for 0-20mA and 4-20mA (SignalType default) the default TransmitterAlarmLow value is 3.

***** If **Scaling** is False the default value for *TransmitterAlarmHigh* = 3428 (3068 for AI [SYS] points)

If **Scaling** is True the default value for *TransmitterAlarmHigh* depends on the chosen SignalType: For 0-5V and 1-5V the default is 5.23 (3.9 for AI [SYS] points); for 0-10V and 2-10V the default is 10.46; for 0-20mA and 4-20mA the default TransmitterAlarmHigh value is 20.93.

Field record handling related to logical symbols

Table 42 on page 437 shows the handling of imported field records related to logical symbols.

For more information on the type of data that is expected in a record, see “Database setup and field properties” on page 410.



Note:

1. For a good understanding of this table you should first read “Creating and importing from an external database” on page 423.
2. As the validity of a field record depends on the value in the Location field *and* on the type of point, you see one column with values per location type.
3. **Markers** carrying binary signals in the application logic are treated as registers in the database tables.

Table 42 Database field interpretation for logical symbols

| Field name & default value | M (marker) | T (timer) | C (counter) | R (register) |
|---|---------------------|---------------------|---------------------|-----------------------|
| <i>NewTagName</i> default = empty | empty | empty | empty | empty |
| <i>Unit</i> default = no text | text | text | text | text |
| <i>SubUnit</i> default = no text | text | text | text | text |
| <i>Status</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Description</i> default = no text | text | text | text | text |
| <i>SafetyRelated</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Size</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ChassisIDAsString</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SlotNumber</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ChannelNumber</i> | default or empty | default or empty | default or empty | default or empty |
| <i>ForceEnable</i> default = False | boolean or empty | default or empty | default or empty | boolean* or empty |
| <i>WriteEnable</i> default = False | default or empty | boolean or empty | boolean or empty | boolean** or empty |
| <i>PowerUpValue</i> default = 0 | 0, 1 or empty | default or empty | numeric or empty | numeric or empty |
| <i>SIL</i> default = no text | text or empty | text or empty | text or empty | text or empty |
| <i>RegisterType</i> default = Word | default or empty | default or empty | default or empty | string or empty |
| <i>SignalType</i> | default or empty | default or empty | default or empty | default or empty |
| <i>Scaling</i> | default or empty | default or empty | default or empty | default or empty |
| <i>BottomScale</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TopScale</i> | default or empty | default or empty | default or empty | default or empty |
| <i>EngineeringUnits</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerBase</i> default = 100ms | default or empty | string or empty | default or empty | default or empty |
| <i>TimerValue</i> default = 1 | default or empty | numeric or empty | default or empty | default or empty |
| <i>Range</i> default = 0 | default or empty | default or empty | numeric or empty | default or empty |
| <i>FaultReaction</i> | default or empty | default or empty | default or empty | default or empty |

Table 42 Database field interpretation for logical symbols

| Field name & default value | M (marker) | T (timer) | C (counter) | R (register) |
|--|----------------------|----------------------|----------------------|----------------------|
| <i>FaultReactionValue</i> | default or empty | default or empty | default or empty | default or empty |
| <i>FieldInputDevice</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SOESetPointLow</i> | default or empty | default or empty | default or empty | default or empty |
| <i>SOESetPointHigh</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmLow</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TransmitterAlarmHigh</i> | default or empty | default or empty | default or empty | default or empty |
| <i>TimerType</i> default = empty | default or empty | string or empty | default or empty | default or empty |
| <i>ComAllocationType#</i> default = empty | “Output” or empty | “Output” or empty | “Output” or empty | “Output” or empty |
| <i>Master#</i> default = empty | string or empty | string or empty | string or empty | string or empty |
| <i>Slave#</i> default = empty | string or empty | string or empty | string or empty | string or empty |
| <i>PLCAddress#</i> default = empty | numeric or empty | numeric or empty | numeric or empty | numeric or empty |

* You can only set *ForceEnable* to True if the register acts as sheet reference for binary/numeric signals.

** You can only set *WriteEnable* to True if the register acts as functional logic.

Log file

The following actions are performed if faults are detected during the import of an external database:

1. *None* of the points are imported and
2. A log file is created

You can use this log file to trace and correct the errors in the external database and then re-import the database.

Sequence of events (SOE)

F

APPENDIX

Sequence of events (SOE) provides the option to detect and record events that indicate or cause deviations from normal process behavior.

This appendix explains the configuration and usage of SOE related to Safety Manager.

| Topic | See |
|---|----------|
| Introduction | page 442 |
| Sequence-of-Event Recording to Experion | page 444 |
| Configuring SOE | page 446 |
| Event Specification | page 450 |
| SOE Characteristics | page 454 |

Introduction

Sequence-of-event recording

Safety Manager contains an integrated sequence-of-event recording (SOE) function, which allows the system to detect and record events that indicate or may cause deviations from normal process operation. Examples of such events are:

- change of state of a valve limit switch,
- process values reaching a critical level,
- changes to maintenance override settings,
- faults in the field (e.g. open transmitter loop),
- faults in input/output interfaces.

Event detection and recording

Safety Manager inspects all defined process quantities once per application cycle for a change of state.

For each changed process quantity an event is recorded in an event buffer that resides within the system.

- The SOE function records events if:
 - an event occurred for a point which is SOE-enabled, (applies to both process points and system points)
 - a force is applied or removed on a point,
- An event record contains:
 - the event (as described in “Event Specification” on page 450),
 - the time stamp of the event (see “SOE Resolution” on page 454), and
 - the SOE ID of the related point (see “SOE ID” on page 443).

Event collection & management

All recorded events are sent to an Event Collection & Management System, such as Experion[™], which may also collect from other event generating systems.

This integrated log in the Event Collection & Management System provides excellent information for post-mortem analysis of abnormal process behavior, in line with the “traceability requirements” of the IEC 61508.

SOE ID

SOE IDs are unique ID numbers assigned to SOE-enabled points and force enabled points. They allow event communication to the Event Collection & Management System with minimal communication overhead.

- If an event occurs for a SOE-enabled point, its SOE ID is contained in the event report. Actual point properties such as point type, tag number, safety relation, etc. are *not* communicated.
- The receiving Event Collection & Management System contains a database with all SOE-enabled point properties. From that database it is able to reproduce all point properties, based on the received SOE ID.

SOE IDs are used for event recording to e.g. Experion[™].

For more information about SOE IDs see “Configuring SOE” on page 446.

SOE logging

SOE channels

Logged events are reported to Event Collection & Management Systems, such as Experion[™], via SOE channels which operate through Safety Manager's communication interfaces.

You can configure one SOE channel per USI.

Time stamp

The time stamp provided in the SOE report is created and reported by the SM Controller detecting the event. This means that e.g. communication delays will not change the reported time stamp of an event.



Attention:

It is mandatory to synchronize the system clocks of *all SOE generating devices in a plant* if all their event reports (including time stamp) are to be collected in one database.

This is even more important if daylight saving is applied by Safety Manager.

For more information about time stamping see “SOE Resolution” on page 454.

Sequence-of-Event Recording to Experion

Introduction

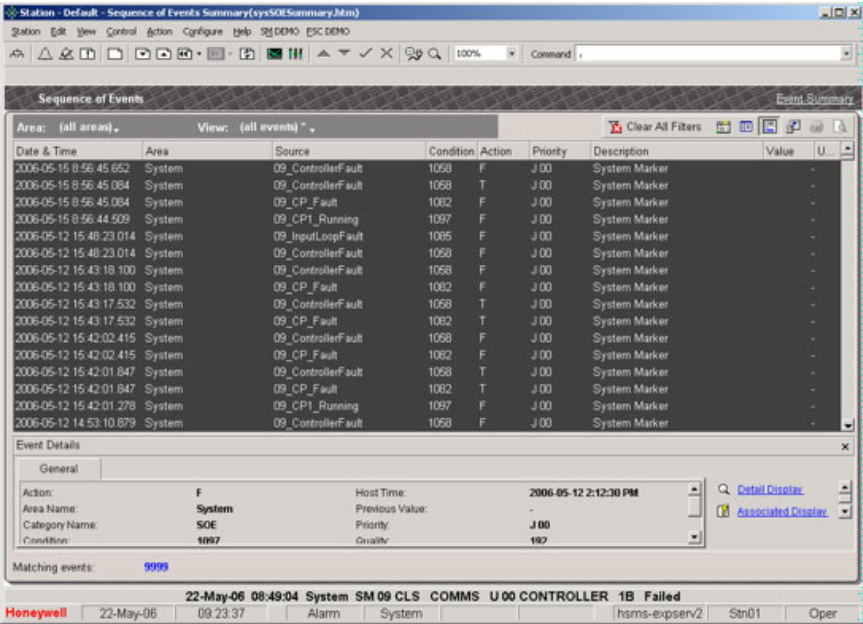
Sequence-of-event (SOE) data generated by Safety Manager can be logged by an Event Collection & Management System such as Experion™.

Using Experion as Event Collection & Management System has the following advantages:

- 1. Full integration, resulting in no compatibility issues.
- 2. Collection of SOE data from multiple Experion related systems in one log file.

Each event on a SOE-enabled point is time-stamped by the SM Controller and reported to the Experion server, where it is incorporated into the standard Experion SOE table. Standard SOE displays are available to view the events as they are reported, as shown in Figure 88 on page 444.

Figure 88 Example of an Experion Station “SOE display”



Configuration

Configuration requirements



Attention:

If the SOE channel configuration is modified later, any SOE data that remains behind in the modified system is lost.

Experion only logs Safety Manager events if points have been assigned to an SOE-only point controller. For configuration details refer to the Experion guidelines.

If you wish to send Safety Manager generated event data to Experion™, the Safety Manager configuration must have:

1. An Experion protocol based communication link between Safety Manager and the Experion server.
2. A shared clock synchronization with Experion.
3. A SOE-only point controller configured in Experion

Setting up SOE to Experion

Setting up sequence-of-event recording to Experion consists of the following steps:

- 1 Enable SOE collection for the Experion server
- 2 Assign a valid SOE ID range for the Safety Manager
- 3 Set the appropriate points SOE-enabled (this assigns a SOE ID to each point).
- 4 Update the point database in the SOE-only point controller.

For details see “Configuring SOE” on page 446.

Supported events

The following event types are recorded and stored by the Experion server:

- Process point events of types DI, DO, AI, and AO,
- Force events of point,
- SOE-enabled system markers and diagnostic markers including
 - diagnostic and system data (user to select which are to be SOE-enabled)
 - SOE buffer full event (always SOE-enabled)

For a more detailed specification of the event types see “Event Specification” on page 450.

Configuring SOE

Configuring SOE basically comes down to:

1. Preparing the communication channel for SOE as described in “Configuring the SOE Channel” on page 446,
2. Using a shared clock synchronization as described in “Synchronizing clock sources” on page 447,
3. Defining the SOE range as described in “Setting the SOE ID Range” on page 447,
4. Set points “SOE-enabled” and allocate SOE sequence numbers as described in “SOE-enabling of points” on page 448, and
5. Import the SOE-enabled points in the Event Collection & Management System as described in “SOE-enabling of points” on page 448.

Configuring the SOE Channel

Before sequence-of-event recording can be used, one or more communication channels need to be identified as "SOE channel" (i.e. the communication channel used by the Event Collection & Management System).

A SOE communication channel must use the Experion[™] communication protocol.

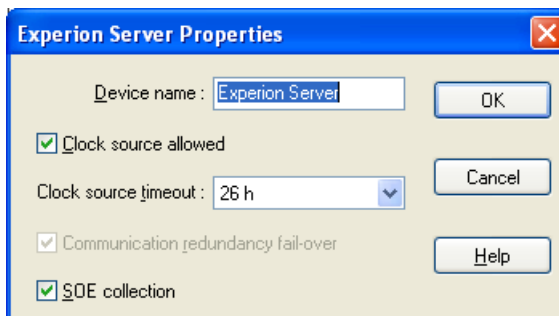


Attention:

1. You can assign one SOE channel per USI.
 2. If a SOE channel configuration is modified, any SOE data that remains behind in the modified system may be lost.
-

To setup a channel for SOE you must:

- 1 Open Network Configurator
- 2 As indicated in Figure 89 on page 447, open the **device properties** of the device(s) you want to configure for SOE, and
- 3 Tick the *SOE collection* box.

Figure 89 Tick *SOE collection* to configure the channel for SOE

Synchronizing clock sources



Caution:

1. Experion can *not* detect if/what daylight saving settings are applied by Safety Manager.
2. Failure to synchronize system clocks and time zones correctly may cause incorrect interpretations when you analyze a SOE log that contains events with time stamps from multiple systems.

All SOE devices must synchronize their clocks to a master clock in order to guarantee that all events in the plant are time stamped from a single (master) clock.

To obtain this situation SM Controllers can synchronize their clocks to:

- a shared plant clock
- the clock of the Event Collection & Management System.

For more about synchronizing clock sources see “Real-time clock synchronization” on page 332.

Setting the SOE ID Range



Note:

1. It is not recommended to overlap SOE ID ranges of various systems in a plant. For more information see this topic.
2. SOE IDs 0 to 15 are reserved and cannot be used.
3. The highest SOE ID that can be assigned is 65534.

The SOE ID range reserves a number of non-overlapping SOE IDs for the following purposes:

1. to define the amount of points that an SM Controller can report events on, which includes:
 - SOE-enabled points and/or
 - Force-enabled points.
(for more on force related events see “Force Events” on page 452.)
2. to identify the SM Controller that generated the events:
 - Assigning different (non overlapping) SOE ranges to the various SOE generating devices makes each SOE ID unique on plant level. This way SOE IDs can also be used to identify the device that generated the event.

Example

Below settings show an example of how to reserve non-overlapping SOE ID ranges that are assigned to the system (node) ID.

- Set **SM Controller_10** to use SOE range 10.000—10.999
 - Set **SM Controller_12** to use SOE range 12.000—12.999
 - Set **SM Controller_63** to use SOE range 63.000—63.999
-

The SOE ID range can be set by opening the **Physical properties** of Safety Manager via Network Configurator.

The range is defined by the values stated in *Min SOE ID* and *Max SOE ID*.

The first *available* sequence number is 16: The first 15 are reserved for system related SOE ID's, such as *SoeBufferFull* and *ControllerFault*.

Related topics:

- “SM Controller properties (physical) - tab: SOE” on page 80

SOE-enabling of points



Tip:

Before you set all point SOE-enabled (which is technically fine), you should first consider if this contributes to the abnormal process behavior analysis. If not, the events generated by points that do not really contribute will only pollute the SOE log.

Safety Manager points need to be prepared for sequence-of-event recording; in other words, they must be "SOE-enabled". Also, they must be provided with a SOE ID.



Note:

SOE IDs are also assigned if points are force-enabled. For more information see "Force Events" on page 452.

The device that receives the SOE data uses the SOE IDs to uniquely identify points.

To make Safety Manager points SOE-enabled, do the following:

- 1 Open the **Point Configurator** in Safety Builder.
- 2 Enable SOE by either:
 - a. Open **Point Properties** and tick the *SOE Enable* box for each individual point you want to enable SOE on.
(A SOE ID is assigned automatically; if the point is an analog you may have to add top and bottom SOE ranges.)
 - b. Import an external point database containing all appropriate settings for each SOE-enabled point.
- 3 Translate and download the updated application

Export SOE-enabled points

After you assigned SOE IDs you must export the relevant points and their properties to your Event Collection & Management System.

Without these properties the Event Collection & Management System is unable to interpret the SOE ID.

- Click **Export Points** in the **Point Configurator** to export points from Safety Manager.
- Consult the user guides of the Event Collection & Management System to determine how to import.

Event Specification



Tip:

Most system and diagnostic events are accessible using system & diagnostic markers. You can treat system and diagnostic markers as points and include them in your event recording. For more information, see “System markers” on page 450.

The SOE function of Safety Manager records the following type of events:

- point events (see “Point Events” on page 450), and
- Force events (see “Force Events” on page 452)

Point Events

A point event is recorded if an event occurs for a process point which is SOE-enabled. To see how to enable SOE on points refer to “SOE-enabling of points” on page 448.

System markers

System markers are points defined by the system. They can be of type DI, DO and M.

When you enable the SOE function of Safety Manager the *ControllerFault* and *SoeBufferFull* system markers are automatically SOE-enabled.

This guarantees that minimal information about the system is included in the SOE report. You are free to expand and set the SOE-enable flag on other system markers as well.

An event occurs if the value of the SOE-enabled system point changes, i.e. Low to High or High to Low.

The event report will contain the point identification, the current point value and the date and time that the event occurred.

Digital inputs (DI)

For point type DI, an event occurs if the application value of the point as applied to the application logic changes, i.e. Low to High or High to Low.

The event report will contain the point identification, the current point value and the date and time that the event occurred.

Digital outputs (DO)

For point type DO, an event occurs if the scan value of the point as applied to the process changes, i.e. Low to High or High to Low.

The event report will contain the point identification, the current point value and the date and time that the event occurred.

Analog inputs and outputs (AI, AO)

An event occurs for analog Point types such as AI and AO if the Point application value moves from one operational area to another.

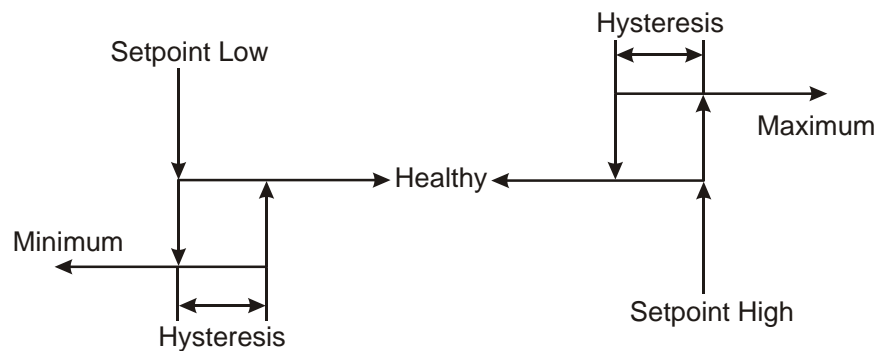
Operational areas

Three operational areas can be defined for analog Points:

1. **Healthy**: this is the normal operational area, between the SOE set point Low and the SOE set point High,
2. **Low**: This is the low-level alarm area, below the SOE set point Low,
3. **High**: This is the high-level alarm area, above the SOE set point High.

Figure 90 on page 451 shows the operational areas defined for event recording of Point types AI and AO.

Figure 90 Event definition for Point types AI and AO



Hysteresis

The hysteresis (i.e. "lag") is 0.5% of the full scale of the analog value.

The absolute value of the hysteresis in engineering units depends on the configuration of the Point and can be calculated.

To calculate the hysteresis in engineering units for channels ranging 0-20 mA, 0-5 V or 0-10 V, the following equation is used:

$$\text{hysteresis}_{0-20} = \frac{10 \times (\text{top} - \text{bottom})}{1638} \quad [\text{engineering units}]$$

To calculate the hysteresis in engineering units for channels ranging 4-20 mA, 1-5 V or 2-10 V, the following equation is used:

$$\text{hysteresis}_{4-20} = \frac{20 \times (\text{top} - \text{bottom})}{2621} \quad [\text{engineering units}]$$

Markers (M)

For point type M, an event occurs if the value of the point changes, i.e. Low to High or High to Low.

The event report will contain the point identification, the current point value and the date and time that the event occurred.

Timers (T)

For point type T, an event occurs if a running timer expires.

The event report will contain the point identification and the date and time that the event occurred.

Counters (C)

For point type C, an event occurs if the counter value changes from non-zero to zero.

The event report will contain the point identification and the date and time that the event occurred.

Force Events



Note:

SOE IDs are always assigned to force-enabled points if Safety Manager is SOE-enabled.

A force event occurs if a process point is forced or a force is removed. The event report will contain the point identification (tag number), an indication if the force was activated or removed, and the date and time that the event occurred.

If the force concerns a point that is SOE-enabled, a point event may occur as well.

SOE Characteristics

SOE Resolution

The occurrence of an event is detected and time stamped within one cycle of the application. The cycle time determines the accuracy of the time stamp.

The time stamp has a resolution of 1 ms.

SOE Buffers and SOE channels

Safety Manager buffers events until they have been reported via the configured SOE channel(s).

SOE channels

SOE channels are used to communicate with Event Collection & Management Systems.



Tip:

To configure a SOE channel, see “Configuring the SOE Channel” on page 446.

SOE channels use the Experion™ protocol communication layer.

You can configure one or more SOE channels per Safety Manager. When configuring SOE channels you:

- must have the Experion protocol configured on the physical layer
- can configure one channel per USI

For information on communication failures related to SOE channels see Communication failures.

Communication failures



Note:

The operation of each communication channel used to report SOE is monitored by Safety Manager.

If a SOE channel goes off-line:

- a diagnostic message is generated, and

- updating event reports via that channel stops. *Event retrieval continues.*

Any incoming events retrieved in that period are stored in the event buffer of the affected SOE channel.

If the off-line SOE channel becomes healthy again:

- the buffered events will be reported to the Event Collection & Management System, and event retrieval and reporting will resume as normal for both channels.

If the off-line SOE channel does not recover in time and the buffer overflows the responses as defined in “SOE buffer characteristics” on page 455 apply.

SOE buffer characteristics

Safety Manager maintains one buffer per SOE channel, each capable of storing at least 500 events.

If an event buffer overflows as a result of an avalanche of events or communication failures with the event collecting & managing device:

1. All subsequent events are ignored for a period of 4 hours. This ensures that the events recorded at the start of a plant upset are kept for post mortem-analysis.
2. Safety Manager only overwrites events in a full buffer if they are older than four hours.

If a buffer overflow occurs, a “SOE buffer full” event is generated and added to the SOE buffer.

Response to anomalies



Caution:

In addition to the “expected SOE anomalies” discussed below the following should be taken into consideration:

- Events that are ready to send (stored in the SOE buffer) are lost when you replace a non-redundant USI on-line.
 - Events generated during an OLM procedure may be lost.
-

The following bullets refer to SOE related anomalies you should expect, and be prepared for:

- SOE buffer not emptied in time and overflows.
See “SOE buffer characteristics” on page 455 for details.
- Unable to access the Event Collection & Management System.
See “Communication failures” on page 454 for details.

F – Sequence of events (SOE)

Diagnostic information

G

APPENDIX

This appendix describes the following types of diagnostic information:

| Topic | See |
|--------------------------------|----------|
| QPP display messages | page 458 |
| Diagnostic messages | page 461 |
| Safety Builder online messages | page 481 |

QPP display messages

The QPP module has a user interface display that informs the user of the status of the Control Processor and all the IO related to it.

The eight-digit display shows one message at a time, and the user can scroll between messages with the use of the buttons on the right-hand side of the display (see Figure 91 on page 458).

Many messages, like diagnostic messages, are divided into sub-messages, called stages (see Table 43 on page 459). The user interface display automatically scrolls through these stages within the current message.

When left alone for 30 seconds, the user interface display returns to the default status message.

The messages are language-independent and include (if applicable) UNICODE languages. This means that messages will be displayed in English as a default, but this depends on the configured language in the Safety Builder.

Figure 91 the user interface display of the QPP-0001 and the QPP-0002

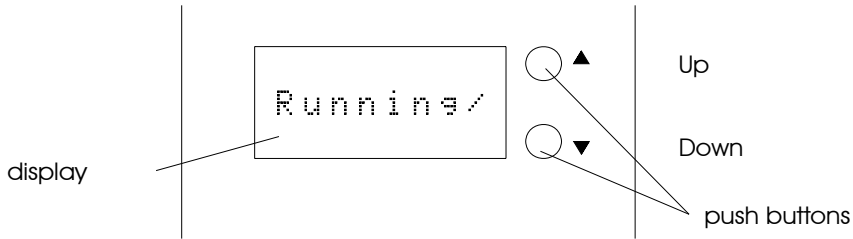


Table 43 Messages displayed by the User Interface Display of the QPP module

| Scroll | Message | Description |
|-----------|--|--|
| Up ↑ | Fail | Shows the number of diagnostic messages (N) |
| | Frc | Shows the number of forced points |
| | Sys | Shows the system ID number |
| | Vb | Shows the battery voltage for this Control Processor in Volts |
| | Vcc | Shows the 5VDC PSU output voltage for this Control Processor in Volts |
| | Tmp | Shows the temperature for this Control Processor |
| | Date | Shows the actual date |
| | Time | Shows the actual time |
| | R #version no.# | Shows the software version number |
| | Default status message* | For details see Table 44 on page 460 |
| Down ↓ | Diagnostic message N | Shows the diagnostic messages that apply for this Controller. |
| | ↓ 1. Chass 2. Slot 3. Module ID 4. Message 1 5. Message 2 | If there are no messages the display shows “Fail 0”. If there are multiple messages the last 32 messages are displayed in chronological order. The last message is shown first. |
| | Diagnostic message N-1 | Select a message with the scroll buttons. When releasing a scroll button on a diagnostic message the display scrolls: |
| | ↓ 1. Chass 2. Slot 3. Module ID 4. Message 1 5. Message 2 | <ul style="list-style-type: none"> the fault location in two steps (chassis and slot), the faulty module in the next step (module ID) the message body in two steps (Message 1 & 2) |
| | ... Diagnostic message 1 | After completing this cycle the display returns to the default status message. |
| | ↓ 1. Chass 2. Slot 3. Module ID 4. Message 1 5. Message 2 | |

* When selecting another display message with the scroll buttons, the display will always return to this message after a time-out.

Table 44 Possible default status messages

| Status | Message* | Alternating with |
|-------------------------------------|----------|------------------|
| Busy with power-on checks | PowerUp | |
| Erasing backup flash memory** | Erase | |
| Busy synchronizing | Sync | |
| Busy loading | Loading | |
| Waiting for download to start | Waiting | |
| Waiting for download to start | Waiting | with Flt |
| Key in IDLE: CP halted | Halt | |
| Key in RUN: CP halted due to faults | Halt | with Flt |
| Key in RUN: CP ready to start | CPReady | |
| Running with faults | Running | with Flt |
| Running no faults | Running | |

* A continues rotating bar or a flashing star on the display indicates that the QPP is operational.

** Appears only after *downgrading* the software in a QPP-0002. Erasing might take several minutes.

Diagnostic messages

**Note:**

Other diagnostic messages, not listed in this book help file, are also possible. If they occur, document the message, message number and circumstances as completely as possible, and contact your local Honeywell affiliate.

This section discusses the diagnostic messages per module.

“About diagnostic messages” on page 462 explains how to interpret the information provided.

Module related diagnostic messages

When applicable, diagnostic messages are sorted by module type:

- “Messages not related to specific hardware modules” on page 464
- “Quadruple Processor Pack modules (QPP-0001 and QPP-0002)” on page 470
- “Communication module (USI-0001)” on page 471
- “Battery and key switch module (BKM-0001)” on page 472
- “Digital input modules (SDI-1624 and SDI-1648)” on page 473
- “Analog input module (SAI-0410)” on page 473
- “Analog input module (SAI-1620m)” on page 474
- “Digital input module (SDIL-1608)” on page 474
- “Digital output module (SDO-0824)” on page 475
- “Analog output module (SAO-0220m)” on page 476
- “Digital output modules (SDO-0448 and SDO-04110)” on page 477
- “Digital output module (SDO-0424)” on page 477
- “Digital output modules (SDOL-0424 and SDOL-0448)” on page 478
- “IO extender (IO-0001)” on page 480
- “Relay output module (RO-1024)” on page 480

Other diagnostic messages

Other diagnostic messages you may be confronted with are:

- “General communication error messages” on page 481
- “Application Viewer messages” on page 481

About diagnostic messages

Message types

Diagnostic messages are of a certain kind and usually include a description, an error code and a message type, indicated by a letter code as shown in Table 45 on page 462.

Table 45 Message types

| Code | Type of message |
|-----------|--|
| E: | Error , which caused Safety Manager to shut down or prevent its start-up. |
| W: | Warning , which indicates a problem has been detected that allows Safety Manager to continue operation (for a limited time period). |
| M: | Message , which provides information on the status of Safety Manager. |

Most diagnostic error messages include information about the cause of the problem and how to best remedy it.

- If this solution does not work try to look for related problems (they may be hard to indicate or do not appear obvious at first glance) and solve those first
- If the problem persists contact Honeywell SMS for advice or try to solve the problem by exchanging the affected modules in the circuitry.

Diagnostic message provide the following information:

- Timestamp
- Chassis number
- Slot number
- Diagnostic type
- Diagnostic details
- Error code
- Hardware module type number
- Diagnostic text (listed in the sections below)

Interpreting diagnostic messages

To interpret diagnostic messages focus on the module ID (see Figure 92 on page 463) and use the table below to find more information about the corresponding message.

Figure 92 Example of an Experion Station “diagnostics display”

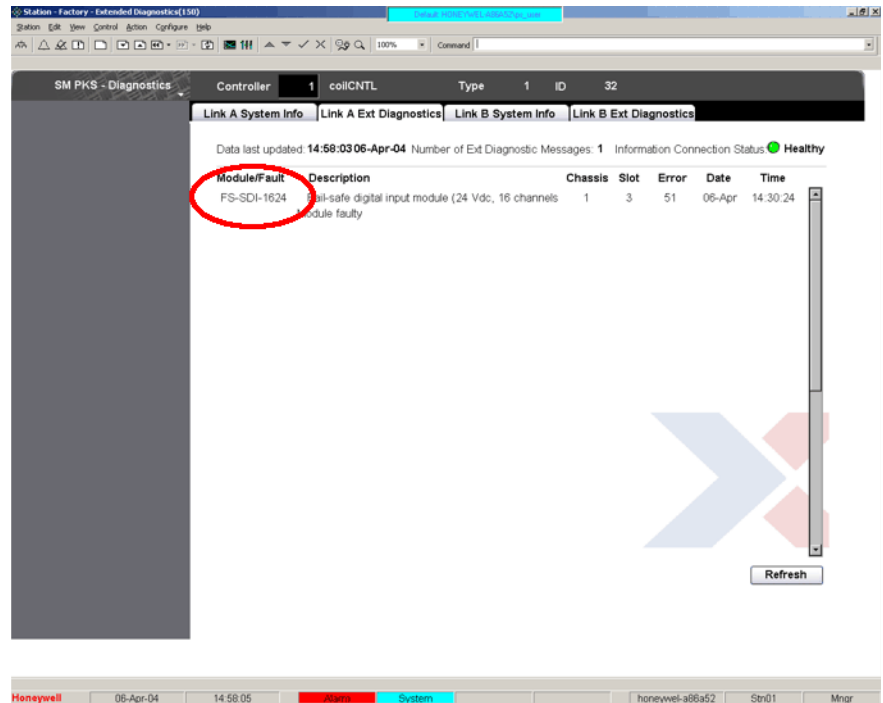


Table 46 Diagnostic messages sorted by Module ID

| Module ID | Refer to... |
|-----------|--|
| BKM-0001 | “Battery and key switch module (BKM-0001)” on page 472 |
| IO-0001 | “IO extender (IO-0001)” on page 480 |
| QPP-0001 | “Quadruple Processor Pack modules (QPP-0001 and QPP-0002)” on page 470 |
| RO-1024 | “Relay output module (RO-1024)” on page 480 |
| SAI-0410 | “Analog input module (SAI-0410)” on page 473 |
| SAI-1620m | “Analog input module (SAI-1620m)” on page 474 |
| SAO-0220m | “Analog output module (SAO-0220m)” on page 476 |

Table 46 Diagnostic messages sorted by Module ID *(continued)*

| Module ID | Refer to... |
|-----------------------|--|
| SDI-1624 SDI-1648 | “Digital input modules (SDI-1624 and SDI-1648)” on page 473 |
| SDIL-1608 | “Digital input module (SDIL-1608)” on page 474 |
| SDO-0424 | “Digital output module (SDO-0424)” on page 477 |
| SDO-0448 SDO-04110 | “Digital output modules (SDO-0448 and SDO-04110)” on page 477 |
| SDO-0824 | “Digital output module (SDO-0824)” on page 475 |
| SDOL-0424 | “Digital output modules (SDOL-0424 and SDOL-0448)” on page 478 |
| USI-0001 | “Communication module (USI-0001)” on page 471 |

Messages not related to specific hardware modules

All forces cleared

All forces are cleared via one action.

Calculation overflow

Calculation yields a result that is out of a specified range.

Solution: check the calculation in the logic of the specified FLD.

Check 24 VDC power supply voltage

A power fluctuation was detected on a 24 VDC power line.

Solution: Check the cause of the power fluctuation. Use the time stamp to detect similarities in process states of other equipment loading the same power grid.

Check 5 VDC power supply voltage

A power fluctuation was detected on a 5 VDC internal power line.

Solution: Check the cause of the power fluctuation. Use the time stamp to detect similarities in process states of other equipment loading the same 24 VDC power grid.

Check IO bus terminator

The IO bus terminator on the Controller backplane is not working as expected.

Solution: replace the IO bus terminator.

Clock source time-out

The external clock source failed to update the SM Controller internal clock within the specified time.

Solution: Check the connection with the external clock source and the update frequency of the external clock source.

Controller too complex to calculate cycle time within configured DTI

Controller configuration is too complex to be executed.

Solution: reduce the application cycle time by:

- increasing the DTI
- reducing system size and/or complexity

Device communication failure

An externally connected communication device has stopped communicating with the SM Controller.

Solution: Check the external communication device, the communication cable and the communication configuration details.

Divide by zero

In a calculation a divide by zero error occurs.

Solution: check the calculations in the logic of the specified FLD.

Download failed**Solutions:**

- repeat the download
- switch the QPP in STOP and back to RUN
- replace the QPP and/or the communication module.

Error code not defined

The error code for this diagnostic message is not defined.

Solution: contact your local Honeywell affiliate.

External communication failure

An error has been detected in the Safety Manager network check.

Solution: investigate the cause of this failure and if necessary contact your local Honeywell affiliate.

ESD input activated

The ESD wiring circuit connected to the Controller backplane has been broken because:

- an ESD button has been pushed or

- there is a wiring defect

Solution: Check the state of the ESD wiring circuit.

Fault Reset

The Reset key switch has been toggled.

Functionality degraded

The non redundant outputs are de-energized by the watchdog or a communication protocol failed.

Solution:

- repair the output that causes the watchdog to de-energize all non redundant outputs
- reset the system to reboot and/or reload the failed communication protocol software or remove and re-insert the communication module.
- replace the communication module

Functional logic diagrams different (OLM)

In a redundant system differences are found in the FLD sheets between the Control Processors during the online modification.

Solution: check if the FLD numbers correspond with the changes you have made.

Illegal argument, e.g. square root of -1

In a calculation an illegal argument is used.

Solution: check the calculations in the logic of the specified FLD.

Illegal counter value

In a calculation an illegal counter value is used.

Solution: check the calculations in the logic of the specified FLD.

Illegal timer value

In a calculation an illegal timer value is used.

Solution: check the calculations in the logic of the specified FLD.

Incompatible Safety Builder version

Application is compiled with another version of Safety Builder than the current one.

Solution: use the correct version of Safety Builder.

Incorrect software version**Solutions:**

- load the correct version
- switch the QPP in STOP and back to RUN to let it synchronize with the other CP
- replace the QPP and/or the communication module

Invalid diagnostic text reference <value>

The generated error code is unknown.

Solution: Contact Honeywell SMS.

Internal communication failure or CP degraded**Note:**

When you manually create shutdowns of one Control Processor -such as during an OLM- you can safely ignore this message: An “internal communication failure or CP degraded” message is *always* generated when loosing communication to the other Control Processor.

An internal communication failure is detected if one of the redundant communication links between the active Control Processors has failed.

Solution: when detecting an internal communication failure the system halts one Control Processor. To resolve the anomaly refer to “Cannot get both CPs on-line simultaneously” on page 37 of the *Troubleshooting and Maintenance Guide*.

Measured and calculated FLD execution difference >10%

The application cycle time went out of range during execution. The cycle time limits are calculated by the SM Controller after loading the Controller file.

Solution: Contact Honeywell SMS.

No differences between applications

A new application version has been loaded, but no differences in the functional logic diagrams and hardware configuration have been detected.

Power supply to field device shorted

Solution: check the point or loop in the field.

Processor module key in IDLE position

Software has just been successfully downloaded to the SM Controller, but the key switch on the QPP module is still in the IDLE position. You need to set it to the RUN position before Safety Manager can start up.

Program execution assertion (output sync)

Solution: Contact Honeywell SMS.

Program update failed

Control Processors are unable to get their software versions synchronized.

Solution: Contact Honeywell SMS.

Redundant input fault

The maximum on time or the maximum discrepancy time of the displayed redundant inputs has expired.

Repair timer expired

The fault that caused the start of the repair timer has not been repaired within the interval time between faults. The Control Processor with the fault stops and the other Control Processor continues.

Repair timer started

An error has occurred and the repair timer has been started.

Solution: repair the error before this timer expires (otherwise a shutdown of the Control Processor or Safety Manager might take place).

Causes that started the repair timer could be:

- (loop) faults on output modules with fault reaction set to Low,
- faults detected on the Force Enable key switch,
- faults detected with non-redundant IO bus extenders.

Safe state initiated by redundant Control Processor

Actual Control Processor is shutdown by other Control Processor.

Solution: check diagnostics of other Control Processor and check other diagnostic messages.

Safe state initiated by software assertion

Solution: contact your local Honeywell affiliate.

SafeNet incompatible embedded software versions

This message can occur if the embedded software of the systems, communicating with each other via SafeNet, are not compatible. You will lose the communication between them if you continue.

Solution: load an old version or continue and lose communication, and upgrade other system to recover communication.

SafeNet incompatible point allocation

The memory map of the systems communicating via SafeNet do not match. Communication will be lost if you continue.

Solution: either perform modification and loose communication or use the old application and redo the modification with the correct memory map.

SafeNet incompatible point configuration

The properties of the SafeNet points do not match.

Solution: change the properties to their correct settings.

Secondary switch off asserted

Actual Control Processor has shutdown other Control Processor.

Solution: check diagnostics of actual Control Processor and check other diagnostic messages.

Spurious watchdog interrupt

This shutdown can be caused by:

- Memory error
Solution: check QPP or COM modules.
- 5 Vdc out of range
Solution: check 5 Vdc power supply.
- Deactivation of SD input
Solution: check if SD input = 24 V or check if the secondary switch off was asserted by the other Control Processor.
- Program runtime error
Solution: contact your local Honeywell affiliate.

The watchdog status is displayed automatically.

Temperature pre-alarm

The temperature in Safety Manager gets critical.

Solution: check the fans, airflow and environmental conditions.

Temperature shutdown

The temperature is out of range.

Solution: check the fans, airflow and environmental conditions.

Quadruple Processor Pack modules (QPP-0001 and QPP-0002)



Tip:

If a QPP appears to be a faulty it is recommended to first test the QPP in a test unit before returning it conform the spare part replacement procedure.

If the QPP appears to be working fine in the test unit, you are requested to contact Honeywell SMS with the original diagnostic message before sending the QPP in as a defective module.

Application program corrupted

A CRC error has been detected in the application program during the start-up check.

Solution: load the Controller file again. If the fault persists after download, replace the QPP module.

Control Processor halt

This message appears if the Key switch is cycled from RUN to IDLE. Note that in a non redundant system this action results in a system shutdown.

Controller halt

This message appears if all Control Processors of the Controller are halted.

Controller not loaded

A new or replaced QPP module does not yet contain an application and cannot be loaded.

Solution: load the Controller file.

CP-CP incompatible point allocation

The positions of the points in the memory of both Control Processors do not match.

Solution: either perform offline modification or use the old application and redo the modification with online modification enabled.

Embedded software corrupted

A CRC error has been detected in the firmware during the start-up check.

Solution: load the Controller file again. If the fault persists after download, replace the QPP module.

Execution time out of range

The application cycle is out of range.

Solution: contact your local Honeywell affiliate.

Idle state initiated due to online modification

This message occurs in redundant configurations, during online modification when the application is loaded in the other Control Processor.

Key switch cycled from RUN to IDLE

The key switch is cycled manually from RUN to IDLE. Note that in a non redundant system this action results in a system shutdown.

Memory error

Not sufficient memory available in the QPP module or the module is faulty.

Solution: replace the QPP module.

Temperature sensor faulty

The specified temperature sensor is regarded faulty.

Solution: replace the QPP module.

Wrong QPP module type placed

A QPP-0001 module is inserted where a QPP-0002 module has been configured.

- Note that this message does *not* apply when inserting a QPP-0002 module where a QPP-0001 has been configured: The QPP-0002 is downwards compatible with the QPP-0001.

Solution: place the correct QPP module type.

Communication module (USI-0001)

Com module inserted

Confirmation that a module is inserted or the Control Processor has (re)started.

After insertion it takes approximately 20 seconds before the COM module communicates with the QPP.

Com module removed

Confirmation that a COM module has been removed.

Communication module faulty

No communication possible with the USI-0001 module.

This message may appear due to communication hang-ups or due to hardware failures.

Solution: pull and re-insert the communication module. If this doesn't help, replace the communication module.

Communication overrun

Too many DI/BI points with location COM have been written to the Control Processor during an application cycle.

Solution: make sure that the number of DI and BI points sent to Safety Manager does not exceed the maximum per application cycle or contact your local Honeywell affiliate.

Communication program corrupted

Solution: reload the Control Processor or re-insert/replace the communication module.

Module faulty

Solution: replace the module.

Too many SOE-enabled points configured

Processing the SOE events takes longer than the configured Controller application cycle time.

Solution: reduce the number of SOE-enabled points until the error does not appear again.

Battery and key switch module (BKM-0001)

BKM removed, transport switch off or fuse blown

This message can have different causes. Either the BKM does not contain a lithium cell, the transport switch for the battery is in the *Off* position, the battery voltage is too low or the battery is empty.

Solution: make sure that the transport switch for the battery is in the *On* position and the battery is OK (see “Check battery” on page 472).

If this does not help you must replace the BKM.

Check battery

The installed battery may be of the wrong type or the battery is drained. For battery details see the *Hardware Reference*.

Solution: replace the battery of the BKM module with an original lithium cell. *Batteries cannot be recharged.*

Force disable fails

There is an issue with the hard wired connection between the QPP and the Force Enable key switch.

Solution: replace the BKM module.

If this does not help, the fault most likely resides in the QPP module; replace the QPP module. If this does not resolve the issue either, contact Honeywell SMS.

Digital input modules (SDI-1624 and SDI-1648)

Input compare error

A discrepancy was detected between the inputs scanned by Control Processor 1 and Control Processor 2.

Solution: check the input signal for fast transients and undefined state (see Figure 93 on page 473). A signal with a undefined state can have a random value.

Figure 93 State of input signals

| |
|-----------------|
| 1 |
| undefined state |
| 0 |

Module faulty

One or more channels of the input module are faulty.

Solution: replace the module.

Analog input module (SAI-0410)

Analog input loop fault(s)

One or more loop faults have been detected. The field sensor(s) may (temporarily) have been out of range or there is/was a (number of) open loop or short circuit(s).

Solution: as multiple channels may have loop faults you must check the **Loop Monitoring** screen to see which channels have loop faults. To find possible causes for analog input loop faults:

- check the value of the field sensor
- check the field wiring.

Input compare error

A discrepancy has been detected between the inputs scanned by Control Processor 1 and Control Processor 2.

Solution: check the input signal for fast transients and undefined state (see Figure 93 on page 473). A signal with an undefined state can have a random value.

Module faulty

The hardware is defective.

Solution: replace the module.

Voltage output short circuit or module faulty

The 26 Vdc output should provide approximately 26 V and the transmitter current should be less than 25 mA.

Solution: if the 26 Vdc output does not provide a high enough voltage: check for short circuits or replace the module. If the transmitter current is higher than 25 mA, reduce the maximum current setting to below 25 mA.

Analog input module (SAI-1620m)

Analog input loop fault(s)

One or more loop faults have been detected. The field sensor(s) may (temporarily) have been out of range or there is/was a (number of) open loop or short circuit(s).

Solution: as multiple channels may have loop faults you must check the **Loop Monitoring** screen to see which channels have loop faults. To find possible causes for analog input loop faults:

- check the value of the field sensor
- check the field wiring.

Internal power-down

There is no internal voltage.

Solution: check the power supply to the module. If no problem can be found, replace the module.

Module faulty, voltage monitoring channel

Discrepancy detected on the module.

Solution: replace the module.

Module faulty

The hardware is defective.

Solution: replace the module.

Digital input module (SDIL-1608)

Earth fault detected

Solution: check the field wiring for earth faults. If no problem can be found, replace the module.

Field device value stuck at

The value of the input field device is stuck at an undefined value.

Solution: check the input signal for slow transients and undefined state (see Figure 93 on page 473). A signal with an undefined state can have a random value.

Internal power-down

There is no internal voltage.

Solution: check the power supply to the module. If no problem can be found, replace the module.

Open loop(s)

One or more loop faults have been detected.

Solution: as multiple channels may have loop faults you must check the **Loop Monitoring** screen to see which channels have loop faults. To find possible causes for digital input loop faults:

- check the field wiring for open loops. If no problem can be found, replace the module.

Module faulty

The hardware is defective.

Solution: replace the module.

Short-circuit

Solution: check the sensor and field wiring for short circuits. If no problem can be found, replace the module.

Digital output module (SDO-0824)

Actual output status invalid

The actual output status is not identical to the calculated value of the application program.

Solution: replace the module.

External power down complete module

If this message is displayed for only one module, the module is faulty.

Solution: replace the module.

If several modules display the same message then there is a common cause for the problem.

Solution: check the fuses or circuit breakers of the external power supply, or check the watchdog signal.

External power down group A

Solution: check the fuses or circuit breakers of the external power supply to channels 1 to 4, or check the watchdog signal.

External power down group B

Solution: check the fuses or circuit breakers of the external power supply to channels 5 to 8, or check the watchdog signal.

Module faulty

A fault has been detected in the common part of the output module.

Solution: replace the module.

Output channel cannot be switched off

Solution: replace the module.

Output compare error

Control Processor 1 calculates another output value than Control Processor 2.

Solution: contact your local Honeywell affiliate.

Short circuit

Solution: check the actuator and field wiring for short circuits.

Analog output module (SAO-0220m)

Actual output status invalid

Solution:

- check the analog output for open loop.
- check the calibration, or replace the module.

Module faulty

A fault has been detected in the common part of the output module.

Solution: replace the module.

Output compare error

Control Processor 1 calculates another output value than Control Processor 2.

Solution: contact your local Honeywell affiliate.

Digital output modules (SDO-0448 and SDO-04110)

Actual output status invalid

The actual output status is not identical to the calculated value of the application.

Solution: replace the module.

External power-down

If this message is displayed for only one module, the module is faulty.

Solution: replace the module.

If several modules display the same message then there is a common cause for the problem.

Solution: check the fuses or circuit breakers of the external power supply or check the watchdog signal.

Module faulty

A fault has been detected in the common part of the output module.

Solution: replace the module.

Output channel cannot be switched off

Solution: replace the module.

Short circuit

Solution: check the actuator and field wiring for short circuits. If no problem can be found, replace the module.

Output compare error

Control Processor 1 calculates another output value than Control Processor 2.

Solution: contact your local Honeywell affiliate.

Digital output module (SDO-0424)

Actual output status invalid

The actual output status is not identical to the calculated value of the application.

Solution: replace the module.

External power down

If this message is displayed for only one module, the module is faulty.

Solution: replace the module.

If several modules display the same message then there is a common cause for the problem.

Solution: check the fuses or circuit breakers of the external power supply or check the watchdog signal.

External power down group A

Solution: check the fuses or circuit breakers of the external power supply to channels 1 and 2 or check the watchdog signal.

External power down group B

Solution: check the fuses or circuit breakers of the external power supply to channels 3 and 4 or check the watchdog signal.

Module faulty

A fault has been detected in the common part of the output module.

Solution: replace the module.

Output channel cannot be switched off

Solution: replace the module.

Short circuit

Solution: check the actuator and field wiring for short circuits. If no problem can be found, replace the module.

Output compare error

Control Processor 1 calculates another output value than Control Processor 2.

Solution: contact your local Honeywell affiliate.

Digital output modules (SDOL-0424 and SDOL-0448)

Correlation between channels

The output channel cannot be switched on or off independently of another channel.

Solution: check if wiring is not crossed between the channels, most likely the return wire is exchanged.

Current detected in output loop

Current has been detected in an output loop, even though the channel is switched off.

Solution: check for short circuits between the channels in the field.

External power-down complete module

If this message is displayed for only one module, the module is faulty.

Solution: replace the module.

If several modules display the same message then there is a common cause for the problem.

Solution: check the fuses or circuit breakers of the external power supply or check the watchdog signal.

Line monitor circuit faulty

The circuit that senses the output loop current is faulty.

Solution: replace the module.

Module faulty

A fault has been detected in the common part of the output module.

Solution: replace the module.

Open loop(s)

One or more loop faults have been detected.

Solution: as multiple channels may have loop faults you must check the **Loop Monitoring** screen to see which channels have loop faults. To find possible causes for digital output loop faults:

- check the field wiring for open loops or,
- check the lead breakage current setting (see the *Hardware Reference*). If no problem can be found, replace the module.

Output channel cannot be switched on

The output is de-energized and cannot be energized.

Solution: replace the module.

Output channel cannot be switched off

The output is energized and cannot be de-energized.

Solution: replace the module.

Output compare error

Control Processor 1 calculates another output value than Control Processor 2.

Solution: contact your local Honeywell affiliate.

Output is incorrectly switched on

The actual output status is 'On', although it should be 'Off' according to the application.

Solution: replace the module.

Short circuit

Solution: check the actuator and field wiring for short circuits. If no problem can be found, replace the module.

IO extender (IO-0001)

Configuration error

The module has been configured but could not be detected in Safety Manager.

Solution: check if the module is placed and check the jumper settings on the IO backplane.

Error code not defined

The error code for this diagnostic message is not defined.

Solution: contact your local Honeywell affiliate.

Module faulty

Solution: replace the module.

IO extender address incorrect or an additional IO extender placed

Solution: check the addressing and allocation of IO extenders.

Relay output module (RO-1024)

Error code not defined

The error code for this diagnostic message is not defined.

Solution: contact your local Honeywell affiliate.

Output compare error

Control Processor 1 calculates another output value than Control Processor 2.

Solution: contact your local Honeywell affiliate.

Safety Builder online messages

This section contains an overview of messages which can appear in the online tools of Safety Builder.

General communication error messages

Illegal command

Information exchange between Safety Builder and SM Controller failed.

Solution: contact your local Honeywell affiliate.

No connection

No communication established with the SM Controller.

Solution:

- a. Check if the cable is plugged into the correct communication port of the Safety Station and Safety Manager.
- b. Check if the communication cable is terminated correctly, has no broken wires, etc.
- c. Check the Network Configurator properties (Controller properties in Physical View and Logical View) in Safety Builder.
- d. Decrease the communication speed (the length of the communication cable may be too long for the communication speed).

Application Viewer messages

Application Viewer does a number of startup tests.

The following messages can appear when you start Application Viewer:

Application configuration has been modified. Please compile and load the application before attempting to start the Application Viewer

Solution: see message description.

Clear not successful on: <tag of point>

The attempt to clear a force status of a point failed. There is a mismatch between the Safety Builder point database and the Controller point database.

Solution: first try to recompile and load the Controller file again. If this message still exists contact your local Honeywell affiliate.

Controller not running or application configuration different from loaded application

Solution: (re)load the Controller file.

Force not successful on: <tag of point>

The attempt to force a point failed. There is a mismatch between the Safety Builder point database and the Controller point database.

Solution: first try to recompile and load the Controller file again. If this message still exists contact your local Honeywell affiliate.

Point not found

Solution: contact your local Honeywell affiliate.

The application can not be viewed. Please check the status of the Controller

Application does not run on the Controller.

Solution: check diagnostics.

Timeout while retrieving status of the Controller

Solution: check the communication with the Controller (see “No connection” on page 481).

Unable to initialize dynamic arrays for point and line data

Solution: contact your local Honeywell affiliate.

Unable to initialize the status of FLD

Solution: contact your local Honeywell affiliate.

Unable to start Application Viewer

The start conditions of the Controller are not correct.

Solution: make the system running. First configure, then compile, load and start the Controller. Now you can start the Application Viewer.

Configuration errors and warnings




This appendix contains all errors and messages that you may get while using one of the Safety Builder configuration tools, as discussed in “Safety Builder configuration tools” on page 41.

The following topics are discussed:

| Topic | See |
|--|----------|
| Application Editor error messages and warnings | page 484 |
| Application Compiler messages | page 493 |
| Application Compiler error messages and warnings | page 494 |

Application Editor error messages and warnings



Notes:

Node (x, y)

Error messages may be followed by the expression **Node (x, y)**. It refers to the FLD coordinates of the error cause. Coordinates indicates the position in x grid points from the left and y grid points from the top of the FLD. The error message also lists the sheet number of the corresponding FLD.

FLD sheet number

If a message contains an FLD sheet number, the cause of the error or warning message may be found on this FLD. If no FLD sheet number is available, it means that the error or warning cause is not situated on an FLD.

Here you will find a list of all error and warning messages related to FLD design using the Application Editor.

The list is in alphabetical order.

A

Attempt to regenerate variable:

| | |
|-------------|---|
| Description | Symbol should have variable assigned. Application Editor will try and regenerate the variable. If it fails, symbol will be erased from FLD. |
| Solution | If regeneration fails, redraw the symbol. |

B

Block contains variable(s) which may not be moved due to On-line Modification.

| | |
|-------------|---|
| Description | The block you want to move contains one or more variables that may not be moved with On-line modification set to Yes. |
| Solution | You cannot do this modification on-line; modify off-line. |

Block does not exist:

| | |
|-------------|--|
| Description | You entered a block name which is not present in your project folder or which is not found in the root of the floppy disk or you entered a file name with extension. |
| Solution | Select a valid block name. |

Block does not fit on screen

| | |
|-------------|---|
| Description | The block you want to copy is too big. |
| Solution | Decrease block size or create more space. |

C

Cannot change register type. Try "Rebuild" option to optimize data file.

| | |
|-------------|---|
| Description | The register type cannot be modified on-line. |
| Solution | Modify off-line |

Communication buffer memory overflow.

| | |
|-------------|--|
| Description | No more communication variables can be allocated. |
| Solution | Allocate more space via Logical View of Network Configurator. |

Constant will not fit in the internal area.

| | |
|-------------|---|
| Description | If the constant symbol is changed to a larger value, the symbol will exceed the IO borders. |
| Solution | Delete the constant value and place a new one. |

Controller memory overflow

| | |
|-------------|--|
| Description | No more addresses available for this type of variable. |
| Solution | Expand the available IO. |

Corrupted block. <block name>

| | |
|-------------|--|
| Description | The block you want to select contains corrupted data. It has been deleted from the disk. |
| Solution | Recreate the block |

D

DISK READ ERROR.

| | |
|-------------|--|
| Description | The program cannot read the complete contents of a file due to an error. |
| Solution | Rewrite the contents to the desired file before attempting another read. |

DISK WRITE ERROR.

| | |
|-------------|--|
| Description | The disk is full or corrupted. The data has not been saved. |
| Solution | Try to free space on the disk and retry with a previous back-up of your application. |

Duplicate reference not allowed.

| | |
|-------------|--|
| Description | You are not allowed to make two sheet transfers to the same destination FLD using one sheet transfer symbol. |
|-------------|--|

| | |
|----------|--|
| Solution | If you want to create two sheet transfers to the same FLD, make a line splitting and connect this signal to a second sheet transfer of that destination FLD. |
|----------|--|

E

Empty block.

| | |
|-------------|--|
| Description | You defined a block which does not contain a symbol that can be manipulated. |
|-------------|--|

| | |
|----------|----------------------|
| Solution | Define another block |
|----------|----------------------|

Empty diagram cannot be copied.

| | |
|-------------|---|
| Description | You entered the name of an undefined FLD. |
|-------------|---|

| | |
|----------|-----------------------------------|
| Solution | Enter the name of an existing FLD |
|----------|-----------------------------------|

Equation file not found: <file name>

| | |
|-------------|---|
| Description | The file name you specified could not be found in the current project folder. |
|-------------|---|

F

File creation failed: <file name>

| | |
|-------------|---|
| Description | Safety Builder attempted to create a file, but that failed (e.g. because the disk is full). |
|-------------|---|

| | |
|----------|---|
| Solution | Check for available disk space and access rights. |
|----------|---|

File opening failed: <file name>

| | |
|-------------|---|
| Description | Safety Builder attempted to open a file, but the file could not be found on the disk. |
|-------------|---|

| | |
|----------|---------------------------------------|
| Solution | Restore a back-up of the application. |
|----------|---------------------------------------|

FLD already exists.

| | |
|-------------|---|
| Description | You must enter the number of an FLD which has not been defined yet. |
|-------------|---|

| | |
|----------|---------------------------|
| Solution | Choose another FLD number |
|----------|---------------------------|

FLD <FLD no.> is corrupted

| | |
|-------------|---|
| Description | Some data which must be present in the sheet database is not found. |
|-------------|---|

| | |
|----------|-----------------------|
| Solution | Contact Honeywell SMS |
|----------|-----------------------|

Function block cannot be referenced.

| | |
|-------------|---|
| Description | You cannot make a sheet transfer to the output side of a function block sheet, as a function block cannot have an off-sheet transfer. |
|-------------|---|

| | |
|----------|-----------------------|
| Solution | Nest function blocks. |
|----------|-----------------------|

I

Illegal application name or block name, or file does not exist.

Description You entered an invalid file name or the name of a non-existing file.

Solution Enter a valid name.

Illegal connection.

Description The connection you tried to make is not allowed, or the signal type is illegal for this symbol.

Solution Make sure the signal types of the corresponding symbols match and use the correct line type to connect the symbols.

Illegal function block input exchange:

Description Two function block input symbols on a function block are exchanged.

Solution Place the function block input symbols as before, or remove the function block call from the FLD. This check is only active if On-line modification has been set to Yes.

Illegal function block output exchange:

Description Two function block output symbols on a function block are exchanged.

Solution Place the function block output symbols as before or remove the function block call from the FLD. This check is only active if 'On-line modification' has been set to 'Yes'.

Illegal input/output.

Description The IO you entered for the diagnostic input is invalid.

Solution Allocate the IO variable to a fail-safe module first. You will also get this message if the data record is corrupted.

Infinite signal cycle.

Description You made a cycle of connection lines which is not allowed.

Input already placed on FLD: <FLD no.>

Description You are not allowed to make two inputs with the same type and tag number per QPP.

Solution Use sheet references to copy the input value to this FLD.

Input/output does not exist: <type + tag no.>

Description The input or output you want to use for the diagnostic input does not exist.

Solution Create and allocate the desired input or output first.

Insufficient memory.

Description You do not have enough internal memory to run the Application Editor.

Solution Try to make room by removing resident programs and drivers from your system. Before you restart the Application Editor, do a hardware reset or switch off your system and switch it on again.

Invalid floating point operation

Description An internal rounding error has occurred and the program will be closed.

Invalid library version. You need version <version>.

Description The library contains a version number which is not compatible with the software version you are using.

Solution Upgrade to the suggested version.

Invalid numeric order in equation table.

Description The input value must be in an ascending numerical order.

Solution Create a new equation table.

Invalid value in equation table.

Description A value defined in the equation file is out of range. The range is 1E-38 to 1E+38.

Solution Create a new equation table.

Inverter must be connected to non-line symbol.

Description An inverter may only be connected to any of the following symbols:

- at the front of logical functions and pulses.
- at the back of timers, pulses and constant boolean signals.
- at the set and reset input of timers and flip-flops.
- at the top and the bottom of rotated logical functions.

Solution Connect to a non-line symbol or use another symbol (e.g. a NAND gate instead of an AND gate).

M

Major block version discrepancy detected. Continue anyway?

Description Safety Builder found major discrepancies when importing FSC logic. The result will not be as expected. Continue at own risk.

Solution Contact Honeywell SMS

Minor block version discrepancy detected. Continue anyway?

Description Safety Builder found some discrepancies when importing FSC logic. The result may not be as expected. Continue at own risk.

Solution Contact Honeywell SMS

N

No more square root functions.

| | |
|-------------|--|
| Description | The number of square root functions per FLD is limited to 10. Another limitation is the execution time of one FLD, which effectively reduces the maximum number of square roots to 1 or 2. |
| Solution | Put the remaining square root functions on a new FLD. |

No more symbols on this FLD or on FLD to be linked.

| | |
|-------------|--|
| Description | The FLD is full, which means that no more symbols can be placed. If you are placing a sheet transfer symbol, it is also possible that the program cannot place the related symbol on the FLD which is referred to. |
| Solution | Save space by decreasing the number of unnecessary line splittings or relocate some logic to a new FLD. |

No sheet version detected. Continue anyway?

| | |
|-------------|--|
| Description | Safety Builder found no sheet version when importing FSC logic. The result may not be as expected. Continue at own risk. |
| Solution | Contact Honeywell SMS |

No space on referenced FLD.

| | |
|-------------|--|
| Description | You attempted to make an FLD transfer to another FLD, but there is no room in the IO area on the referenced FLD to place the related symbol. |
| Solution | You might create new space by moving the IO closer to each other. |

Not enough entries in equation table.

| | |
|-------------|---|
| Description | The minimum number of entries in an equation table file is 3. |
| Solution | Add more reference points to the equation table. |

Not enough free disk space.

| | |
|-------------|-----------------------|
| Description | Your disk is full. |
| Solution | Free some disk space. |

Number of input bits must be a multiple of 4 for decimal IO.

| | |
|-------------|---|
| Description | A BI or BO with hexadecimal data representation must have a number of data bits which is a multiple of 4. |
| Solution | Use the Point Configurator of Safety Builder to change the number of data bits. |

O

One or more illegal symbols deleted.

Description After a block type change, some symbols are incompatible with the new block type, or they have an illegal position. These symbols are deleted.

Solution Contact Honeywell SMS.

Output already placed on FLD: <FLD no.>

Description You are not allowed to make two outputs with the same type and tag number.

Solution Use sheet references to reroute the logic to the FLD containing the output and connect there.

P

Program will be terminated

Description An internal error has occurred and the program will be closed.

Solution Contact Honeywell SMS.

R

Reference to non existing FLD

Description A marker or sheet reference refers to a non existing FLD

Solution Delete and reinstall the marker or reinstall a backup

Reference to mnemonic sheet or non-logic sheet is not allowed.

Description You cannot transfer a signal to a non-logic sheet or a mnemonic sheet.

S

should exist.

Description A nonexisting sheet should exist.

Solution Reinstall a backup

Symbol is corrupted and will be deleted.

Description A corrupted symbol or sheet has been detected and this will be removed.

Solution Reinstall a backup

Symbol is too large to move.

Description Symbols which are larger than the screen cannot be moved.

Solution Adjust the scaling of Application Editor.

Symbol library corrupted.

Description The symbol library is corrupted and needs to be reinstalled.

Solution Reinstall a backup of the application or reinstall the Safety Builder

Symbol overlap.

Description You attempted to place a symbol on a location which is already occupied by another symbol.

Solution Try a new position.

Symbol will be erased from FLD.

Description An attempt was made to regenerate the variable. As this failed the symbol will now be erased from FLD. See also "Attempt to regenerate variable:" on page 484.

Solution Redraw the symbol.

Syntax error in equation table.

Description The equation table contains an illegal entry or text.

Solution Create an equation table following the prescribed format.

T

Text too long.

Description The text is too long to be placed on the screen.

Solution Modify the text, or change the scale and/or number of strokes.

This FLD has wrong block type or does not exist.

Description The FLD number you entered is invalid because it does not have the required block type, e.g. you want to place a function block but you specified the number of an empty FLD or a program block FLD.

Too many connection lines.

Description You made a path of connection lines which contains too many lines.

Solution Place a buffer inbetween.

This type of symbol cannot be placed on this FLD anymore.

Description You have reached the maximum amount of symbols of this type that can be installed on a single FLD.

Solution Expand your logic to another FLD

Too many entries in equation table.

| | |
|-------------|---|
| Description | The maximum number of entries in an equation table file is 200. |
| Solution | Remove items from the equation table until the number of entries is lower than 200. |

U

Unknown error type

| | |
|-------------|---|
| Description | An undefined error has occurred and the program will be closed. |
|-------------|---|

V

Variable may not be moved due to On-line Modification.

| | |
|-------------|--|
| Description | This type of variable may not be moved with On-line modification set to Yes. |
| Solution | Set On-line modification to No and <i>modify off-line</i> . |

Variable not found in IO data file:

| | |
|-------------|---|
| Description | The variable is found on the current FLD, but it does not exist in the IO data file. Safety Builder will try to regenerate the variable. If this is not successful, the variable will be erased from the FLD. |
|-------------|---|

W

Wrong block type.

| | |
|-------------|--|
| Description | The FLD you want to copy has a different block type than the FLD you are editing. This is not allowed. |
| Solution | Use FLD properties to adjust the block type. |

Application Compiler messages



Note

If the Application Compiler detects an error, no SM Controller File is generated. Normally when you start the Application Compiler, it automatically deletes the previous SM Controller File. In case of errors the previous SM Controller File will not be deleted.

During compilation the Application Compiler of Safety Builder creates a log file which lists:

- 1 All errors found in the FLDs and databases.
- 2 All generated warnings.
Warnings refer to instances where the code is syntactically correct but will probably not perform the intended function.
- 3 Some compilation data, for example the number of markers in the application.

When applicable the Application Compiler may indicate the coordinates of a symbol and/or the sheet number to which the message applies.

Node (x, y)

Error messages may be followed by the expression **Node (x, y)**. It refers to the FLD coordinates of the error cause. Coordinates indicates the position in x grid points from the left and y grid points from the top of the FLD. The error message also lists the sheet number of the corresponding FLD.

FLD sheet number

If a message contains an FLD sheet number, the cause of the error or warning message may be found on this FLD. If no FLD sheet number is available, it means that the error or warning cause is not situated on an FLD.

Application Compiler error messages and warnings

Here you will find a list of all error and warning messages related to compiling the application using the Application Compiler.

All the error message text listed that is encapsulated between the less-than and greater-than signs < > are to be replaced by actual strings or values.

| | |
|---------|---|
| Example | <p>Analog IO allocation error: <type> <tag number></p> <ul style="list-style-type: none">• <type> is to be replaced by the point type, being either: AI, DI, BI, AO, DO, BO• <tag number> is to be replaced by the tag ID of that point. |
|---------|---|

The list is in alphabetical order.

A

A functional logic diagram must contain at least one output symbol.

| | |
|-------------|--|
| Description | At least one output symbol (output, BO, off-sheet reference, etc.) is required on each functional logic diagram. |
| Solution | Make sure that each FLD contains at least one output symbol or change the FLD type to <i>comment block</i> . |

Analog IO allocation error: <type> <tag number>

| | |
|-------------|--|
| Description | The specified analog point has not been properly allocated to the hardware (chassis, slot, channel is not specified). |
| Solution | Use the Point Configurator to allocate the point. If the FLD number of the point is 0 (zero), the point is not used in the FLDs and may be deleted. You can use the Point Configurator (filter on “ non allocated ”) to find all points that were not properly allocated. |

Application address of point "<tagnumber>" (<type>) does not match with input block configuration.

| | |
|-------------|---|
| Description | The application address of the point does not match the buffers in the database due to an incorrect or missing buffer assignment. The database probably contains errors and is corrupted. |
| Solution | Repair or rebuild the application or contact Honeywell SMS. |

Application address of point "<tagnumber>" (<type>) is not in the correct buffer.

| | |
|-------------|---|
| Description | The application address of the point does not match the size of the application buffer. The database probably contains errors and is corrupted. |
| Solution | Repair or rebuild the application or contact Honeywell SMS. |

Application address of point "<tagnumber>" (<type>) is not located on an even byte address.

Description The application address of the point starts at an odd address in the application buffer. Addresses for the SM Controller must start at even addresses. The database probably contains errors and is corrupted.

Solution Repair or rebuild the application or contact Honeywell SMS.

Application Compiler out of space.

Description The number of mnemonics or the number of found symbols in the FLD cannot be stored internally.

Solution Try to optimize the FLD with regard to the number of symbols needed for particular functions.

Try to change the partition of your total functional logics design in such a way that fewer functions are needed per FLD.

Use the Application Editor of Safety Builder to remove some symbols.

Application contains too many <symbol type>

Description Too many symbols of the specified type have been used in the application.

Solution Use the Application Editor of Safety Builder to remove some symbols.

Application too large to fit on controller memory

Description The application has grown beyond the available memory space on the QPP module.

Solution Optimize your application or contact Honeywell SMS.

C

Called block is no function block: <function block>

Description A call is made to an FLD which is not a function block FLD.

Solution Delete the call in the calling FLD.

Called block is no or incorrect equation block: <equation block>

Description The referenced diagram is not an equation block diagram.

Cannot change register type. Try "Rebuild" option to optimize data file.

Description There may be a mismatch between register type defined in logic and point definition. Cause can be registers may have been allocated on different locations.

Solution Use the Database Rebuilder of Safety Builder to synchronize the registers.

Clock source configuration error

Description A clock source is specified in a Safety Manager that is not connected with a physical connection. In the Network Configurator clock source is not configured properly.

- Solution In Network Configurator check the device properties on the following:
- Make sure that clock source is allowed.
 - Make sure that a logical connection with the device exists.

Clock source priorities configuration error

Description Clock source priorities are not specified for the SM Controller. It is obligatory to define 3 sources in order of priority.

Solution Use the Network Configurator of Safety Builder to specify the Safety Manager properties.

Com module configuration has unexpected names

Description The identification of Com modules is inconsistent, the database may contain errors.

Solution Use the Database Rebuilder of Safety Builder to recover inconsistencies.

Compilation completed.

Description The Application Compiler has checked all FLDs and all data in the databases without encountering serious errors.

Configured Diagnostic Test Interval (s): <time>

Description This is the Diagnostic Test Interval as specified in the database (in seconds).

Corrupted data: <type> <tag number>

Description Some properties of the specified point are corrupted.

Solution Use the Point Configurator to change the properties of the point.

Corrupted data detected.

Description The current installation FLD contains a corrupted record.

Solution Use the Database Rebuilder to regenerate the configuration.

Corrupted file: <file name>

Description A (temporary) file which was created by the Application Compiler is corrupted.

Solution Check the integrity of your disk with a utility such as **CHKDSK**, remove the bad sectors from your disk and restart the compilation.

Could not create FLD transfer index file: <file name>

Description An old index file still exists.

Solution Cleanup your **temp** folder in Windows.

Counter allocation error: <type> <tag number>, <type> <tag number> (<address>)

Description The counter has an address, which is already used by one or more other counters.

Solution Use the Database Rebuilder to check the addresses of all points.

Count-up or count-down not allowed for a float register.

| | |
|--|---|
| Description | The count-up or count-down operation is only valid for integer-type registers (byte, word or long). |
| Solution | Use the Application Editor to change the FLDs. |
| Current application version: <version> | |
| Description | If the compilation is complete, the version of the software is listed. |

D

Data error in FLD <number>

| | |
|-------------|---|
| Description | The currently compiled FLD contains a corrupted record. |
| Solution | Use the Application Editor to see if all symbols are still present and correct. |

DCS address allocation error detected

| | |
|-------------|---|
| Description | Two points communicate to the same system using the same DCS address. |
| Solution | Use the Point Configurator to remove duplicate address. |

Digital IO allocation error: <type> <tag number>

| | |
|-------------|--|
| Description | The specified digital point has not been properly allocated to the hardware (chassis, slot, channel has not been specified). |
| Solution | Use the Point Configurator to allocate the point. If the FLD number of the point is 0 (zero), the point is not used in the FLDs and may be deleted. You can use the Point Configurator (filter on “ non allocated ”) to find all points that were not properly allocated. |

DISK READ ERROR: <file name>

| | |
|-------------|--|
| Description | An unsuccessful attempt was made to read data from the specified file. |
| Solution | Check the integrity of your disk with a utility such as CHKDSK , remove the bad sectors from your disk and restart the compilation. |

DISK WRITE ERROR: <file name>

| | |
|-------------|--|
| Description | An unsuccessful attempt was made to write data to the specified file. |
| Solution | Check the integrity of your disk with a utility such as CHKDSK , remove the bad sectors from your disk and restart the compilation. |

Duplicate FLD transfer in index file: <tag number>

| | |
|-------------|---|
| Description | The index file is corrupted. |
| Solution | Use the Database Rebuilder to rebuild the index file. |

Duplicate off-sheet reference on FLD: <FLD>

| | |
|-------------|--|
| Description | An off-sheet reference with the specified point number has been placed on one FLD twice. |
| Solution | Use the Application Editor to remove one reference. |

Duplicate on-sheet reference on FLD: <FLD>

Description An on-sheet reference with the specified point number has been placed on one FLD twice.

Solution Use the Application Editor to remove one reference.

Duplicate point number on FLD: <type> <tag number>

Description A point with the specified tag number has been placed on one FLD twice.

Solution Use the Application Editor to remove one tag number.

E

Error in link configuration to system

Description A logical connection is made to the same system the connection originates from.

Solution Use the Database Rebuilder to resolve the connection.

Error in FLD:

Description The currently compiled FLD contains a corrupted record.

Solution Use the Application Editor to check the FLD.

F

Fatal error. Compilation aborted: <time> <date>

Description This message is printed if for some reason the compilation process cannot continue. Possible reasons are disk full or insufficient memory.

File creation failed: <file name>

Description The specified file could not be created. For example, the disk may be full or the number of open files has been exceeded.

Solution Clean your disk, i.e. delete unused files or save currently unused files to a removable storage medium (e.g. a diskette), and delete them from your hard disk.

Solution Use a system with a larger disk capacity.

File opening failed: <file name>

Description An attempt was made to open the specified file, but it was not found or could not be opened.

Flasher frequency too high to work properly

Description Flasher frequency is higher than the response time of the application.

Solution Use an appropriate flasher.

FLD contains too many <symbol type>

Description Too many symbols of the specified type have been placed on an FLD.

Solution Use the Application Editor to remove some symbols or split the functional logic over two FLDs.

FLD is corrupted: <FLD>

Description The specified FLD contains corrupted data.

Solution Use the Application Editor to load the FLD, and then delete it.

FLD is full. Function block cannot be corrected.

Description An FLD contains too many symbols which require a lot of physical space on a station.

Solution Use the Application Editor to edit the FLD (e.g. split into more FLDs).

FLD reference not found on FLD: <type> <tag number>

Description The FLD reference with <tag number> is found on one FLD but not on a referenced FLD.

Solution Use the Application Editor to replace the reference.

FLD too big or nesting too deep. FLD time: <time>

Description The execution time of the FLD is too large because function blocks have been nested too deep or there are too many time-consuming functions.

Solution In the Application Editor change the FLDs so that fewer functions or other functions are needed. Change the nesting of the function blocks, since too many function block calls can cause the execution time to become too large. Split the FLD into two or more FLDs. Particularly time-consuming functions are square root.

FLD transfer expected to be directly connected to IO symbol. <type> <tag number>

Description You defined a service text that is identical to the point number of an IO symbol, but no direct connection exists.

Solution Use the Application Editor to change the service test or make a direct connection.

Function block diagram in program block area: <no.>

Description The FLD number of a program block must be at least two less than the FLD number of the first function block.

Solution Use the Application Editor (renumber option) to shift down the program block or to shift up the function block. Check all calls to this function block.

Function block diagram missing: <FLD>

Description The function block which is called at the specified FLD is not available in the project folder (file is not found).

Solution Delete the function block on the calling FLD or restore the function block diagram.

Function block diagram must contain at least one function block output.

Description A function block must have a function block output, otherwise it is of no use in the functional logic diagrams.

Solution Place a function block output or delete the FLD.

Function block has no inputs

Description An FLD contains an function block without connecting to one of its inputs.

Solution If you add a function block with inputs to an FLD, you must connect at least one input of the function block. The following solutions exist:

1. Connect the input to a constant value
2. Remove all inputs from the function block

Function block input not connected. Function block input sequence number: <seq. no.>

Description An input of a function block has not been connected to a signal in the FLD. This is allowed but a warning is nevertheless given, because it might be not intended. The input value will be zero during execution.

Function block symbol corrupted.

Description A function block symbol has been found to be corrupted.

Solution Use the Application Editor to delete and replace the corrupted function block.

Function change failed.

Description The FLD contains too many point of the specified type (markers, counters, timers or registers).

Solution Use the Application Editor to edit the FLD (e.g. split into more FLDs).

I

Identical source and destination are not allowed.

Description The source FLD and destination FLD for a sheet transfer is identical, which is not allowed.

Solution Make sure that the source and the destination FLD in a sheet transfer are different.

Illegal address: <type> <tag number>

Description The specified point in the database has an illegal address.

Solution Rebuild the point database via the Database Rebuilder or (re)assign the logical connection address.

Illegal bit number: <bit no.>

Description The bit number is corrupted.

Solution Rebuild the point database via the Database Rebuilder or (re)assign the logical connection address.

Illegal connection: Node (x, y)

Description A signal line has been connected to a symbol at a point where it is not allowed, or the signal line is not a valid signal type. Function blocks and registers have predefined input and output positions.

Solution Use the Application Editor to change the connection.

Illegal constant: <type> <tag number>

Description The value of the constant is not allowed (e.g. a negative constant is loaded to a counter).

Solution Use the Application Editor to change the constant.

Illegal counter value: Node (x, y)

Description The value which will be loaded into the counter is illegal.

Solution Use the Application Editor to change the constant value or change the range of the counter.

Illegal function block call: <function block>

Description The function block called has a higher or an equal FLD number than the current FLD.

Solution Remove the function block from the current FLD. Renumber the function block to an FLD with a number higher than the current FLD number. Place the function block again on the current FLD.

Illegal function block input exchange.

Description Two function block inputs have been exchanged illegally.

Solution Use the Application Editor to place the symbols as before.
Only active if online modification is set to 'Yes'.

Illegal function block output exchange.

Description Two function block outputs have been exchanged illegally.

Solution Use the Application Editor to place the symbols as before.
Only active if online modification is set to 'Yes'.

Illegal input signal type of function block: <function block> Node (x, y)

Description The signal type of the register on the FLD cannot be converted to the signal type of the function block input. The calling FLD long register cannot be connected to a word register.

Illegal name of application stored in database: <appl. name>

Description The name of the current application has not been specified for the current system number. For example, the current application is TEST_1. The application name for system 1 in the current database is, for example, DEMO. This will happen if an application has been renamed "outside" Safety Builder (e.g. using Windows Explorer).

Illegal signal type(s): Node (x, y)

Description The signal type is illegal for the symbol to which it is connected. For example, a signal of type Long cannot be connected to a counter or timer.

Description The types of the signal coming from the FLD to an internal off-sheet symbol (i.e. decimal marker) do not match and conversion is not allowed for internal symbols.

Solution Use the Application Editor to change the signal type.

Illegal symbol for this block type: <block type>

Description The FLD contains a symbol which should not be present in an FLD with the specified block type.

Solution Use the Application Editor to delete the symbol.

Illegal value: <type> <tag number>

Description The value of the point (timer or counter) is less than or equal to zero, or greater than the maximum value (counter maximum = 8191).

Solution Use the Application Editor to change the point.

Inaccurate scaling specified for analog input:

Description The difference between the bottom and top scale value is too small.

Solution Use the Point Configurator to change the scaling values of the specified point.

Infinite signal cycle: Node (x, y)

Description A signal line has been connected to itself (perhaps via several other FLDs), creating a loop.

Solution Use the Application Editor to delete the loop.

Input blocks have overlapping addresses.

Description The buffers for marker and/or register blocks of logical connections of the SM Controller have overlapping address ranges. The database probably contains errors and is corrupted.

Solution Repair or rebuild the application or contact Honeywell SMS.

Invalid field input device configured for <tag number>

Description The variety of field input device types (NAMUR etc.) of one input module is limited. The identified point is connected to an invalid field input device type, or too many different field input device types are defined on the allocated module.

Solution Use the Point Configurator to allocate the point to another input module or to change the field input device type.

Invalid FLD reference: <tag number>

Description The FLD reference with the specified point is not correct (not found in the point data file or found twice on FLDs).

Solution Use the Application Editor to remove the reference.

Invalid input block start address for logical connection "<master node - slave node>".

Description The buffers for the marker and/or register blocks contain an invalid value for the buffer's start address. The database probably contains errors and is corrupted.

Solution Repair or rebuild the application or contact Honeywell SMS.

Invalid IO for diagnostic status.

Description The diagnostic input is not assigned to a hardware allocated point.

Solution Allocate the point to a hardware channel or assign the diagnostic input to an existing hardware allocated point.

Invalid <marker/register type> size for logical connection "<master node - slave node>".

Description The block size of the specified type is not a multiple of 4.

Solution Reconfigure the size in Network Configurator.

Invalid library version. You need version <version>

Description The library has a different version than the Application Compiler, but cannot be converted.

Solution Use a Safety Manager of the specified version or reinstall the software.

Invalid numeric order in equation table.

Description The input value defined in the equation table is not in ascending numerical order.

Solution Make sure the input value is in ascending numerical order.

Invalid <property name> on <object name> "<object id>" configured.

Description A property or value has been defined that is invalid.

Solution Change the indicated property or value.
If that does not help contact Honeywell SMS.

Invalid SafeNet block size for logical connection "<master node - slave node>".

Description The total size of marker and register bytes on the referred SafeNet link of this SM Controller is larger than the maximum allowed of 2000.

Solution Reconfigure sizes in Network Configurator.

Invalid safety relation configured at (chassis, slot): <chassis>, <slot>

Description The module at the specified location has a `Safety-related` attribute that is set to `Yes` and a `Tested` attribute that is set to `No`, which is an invalid combination.

Solution Use the Point Configurator to reset the `Safety-related` attribute and `Tested` attribute of the specified module.

Invalid SOE ID detected for <tag number>

Description The given point has a SOE ID, but the SM Controller has no specified SOE range or the point is not SOE-enabled or Force-enabled.

Solution Remove the SOE ID via the **Point Configurator**, rebuild the application or contact Honeywell SMS.

Invalid value in equation table.

- Description A value defined in the equation table is out of range.
- Solution Make sure the value is in the legal range (1E-38 to 1E+38).

Invalid/unknown IO Module configured

- Description The IO module configured is not supported by the SM Controller.
- Solution Use the Hardware Configurator to remove the invalid IO module.

IO buffer full: <type>

- Description The buffer used for digital or analog IO is full.
- Solution Use the Hardware Configurator of Safety Builder to delete some IO modules of the specified type.

IO Module address(es) have been changed.

- Description This warning will occur if the Application Compiler detects invalid addresses of IO modules in the database. IO points which are allocated to these modules will have other addresses.

IP address for NTP clocksource "<device name>" is not valid or not specified: <IP address>.

- Description The IP address of the configured clock source is either not filled in or it's value is already in use by another node in the Plant.
- Solution Set a valid IP address in the **device properties** dialog of the clock source in the Network Configurator.

Isolated symbol: Node (x,y)

- Description A symbol has been found without any direct or indirect output connection to an off-sheet symbol.
- Solution Use the Application Editor to connect the symbol or delete it.

L

Library corrupted: <library name>

- Description The specified library file is corrupted.
- Solution Reinstall Safety Builder from the CD ROM.

Library not found on disk: <library name>.SYM

- Description The library used to create the functional logic diagrams cannot be found in the Safety Builder application folder (<InstallFolder> by default).
- Solution Reinstall Safety Builder from the CD ROM.

Load and value must both be connected or not connected: Node (x, y)

- Description If you have a load function, you need a value to be loaded into the register. If you do not have a load function, no value is needed.
- Solution Make sure a value is loaded into the register.

Logic sequence too complex: Node (x,y)

Description The Application Compiler has memory problems when compiling the sequence to the specified node point.

Solution Use the Application Editor to split the functional logic diagrams into simpler or shorter sequences.

Logical connection expected for <tag number>

Description The identified point requires one (or more) logical connections to a device or a Controller.

Solution Add a logical connection to this point or change the location of the point.

M

Mathematical operation of <float> signal type with <integer> type:

Description In the Safety Manager Application a mathematical operation has to be performed between two different signal types (e.g. float and integer). A warning is given if such an operation uses more processor time than the same operation between two signals of the same type.

Solution Change one of the two types to make them both the same.

Maximum delay time on communication link (COM, Chan.): <value> ms

Description This message is given for each multidrop communication channel in a communication server Safety Manager Application. It shows the maximum response time (in ms) of that channel. This information helps the user decide how to balance overloaded communication channels.

Mismatch between data from FLD database and configuration database: <tag number>

Description The information for the specified point number (typically used by a function block) contained in the FLD database does not match the corresponding information in the Safety Manager configuration database.

Solution Use the Application Editor to remove the function block that uses the specified point number from the affected FLD and place it again.

Missing FLD: <appl. name>.<FLD>

Description The file that contains the FLD cannot be found on disk.

Solution Repair or rebuild the application or contact Honeywell SMS.

Missing input block start address for logical connection "<master node - slave node>"

Description The logical connection has marker and/or register blocks assigned but no corresponding buffers could be identified in the database. The database probably contains errors and is corrupted.

Solution Repair or rebuild the application or contact Honeywell SMS.

Missing signal or unconnected signal line: Node (x, y)

Description A signal line which should be connected has not been connected at node point (x, y).

Solution Use the Application Editor to connect or delete the line.

Missing SOE ID for <tag number>.

Description A SOE range was specified in the SM Controller and the given point is SOE-enabled or Force-enabled but lacks a valid SOE ID.

Solution If a SOE range is specified, *all* SOE-enabled and/or Force-enabled points must be given a SOE ID: Apply a SOE ID to the given point.

More than one signal at a node: Node (x, y)

Description Two independent signals may not be connected.

Solution Use the Application Editor to disconnect them.

Multiple IO allocation error: <type> <tag number>

Description This means that a point has not been properly allocated to the hardware for all necessary IO bits (chassis, slot, channel has not been specified).

Solution Use the Point Configurator to allocate the point. If the FLD number of the point is 0 (zero), the point is not used in the FLDs and may be deleted.

You can use the **Point Configurator** (filter on “**non allocated**”) to find all points that were not properly allocated.

N

Network overload detected for (COM module, channel.): <COM> <channel>

Description This error message will typically appear if the time-out configured for the SafeNet configuration is too short for the amount of data transferred within the network.

Solution Use the Network Configurator to increase the communication time-out.

Network too large for clocksource "<device name>".

Description More than one physical network has been attached to the clock source device. A clock source device may be connected to only one network.

Solution Check the physical network configuration in Network Configurator.

No application connected for COM chan. (COM module, chan.): <COM> <channel>

Description The specified channel from the communication module in the specified Control Processor with the specified sequence number has been defined as an external Safety Manager protocol, but no other application has been specified.

Solution Use the Network Configurator to specify the communication link.

No logical connection to a Safety Builder configured

Description No connection is found to connect the Safety Station to. (Mandatory to load the SM Controller.)

| | |
|--|---|
| Solution | Use the Network Configurator to create a logical connection to a Safety Builder. |
| No hardware specified. | |
| Description | The database has not been configured; no hardware has been specified. |
| Solution | Use the Hardware Configurator to specify the hardware of the application. |
| No load signal, so a count signal and clear signal must be connected: <type> <tag number> | |
| Description | If you do not load a register, you must at least use a count-up or a count-down in combination with a clear, otherwise the register is of no use. |
| Solution | Make sure all conditions are met to use the register. |
| No logical connection for specified clock source | |
| Description | A clock source is specified in a SM Controller that is not connected with a logical connection. |
| Solution | In Network Configurator check the device properties on the following: <ul style="list-style-type: none"> • Make sure that clock source is allowed. • Make sure that a logical connection with the device exists |
| No master system detected for (COM, Ch): <COM module>, <channel> | |
| Description | The slave channel specified does not communicate with an external (master) system. |
| Solution | Use the Network Configurator to add a master application to the specified channel. |
| No protocols specified for COM module (COM module): <seq.> | |
| Description | The protocol of channel A and channel B from the communication module in the specified Control Processor with the specified sequence number have not been set (Protocol = undefined). |
| Solution | Use the Network Configurator to specify a protocol, or remove this communication module. |
| No SOE collector detected. | |
| Description | The compiled SM Controller has a specified SOE ID range but no logical connection to a SOE collecting device was configured. |
| Solution | Create a logical connection to a SOE collecting device. |
| Not enough disk space found. Required disk space: <MB> | |
| Description | The Application Compiler requires <MB> megabytes of hard disk space. |
| Solution | Free disk space by deleting files that are no longer needed. |
| Not enough memory to execute required compilation function(s). | |
| Description | The Application Compiler needs more memory to execute the compilation process. |
| Solution | Free memory by closing any other applications that are running. |

Number of data memory bytes: <number>

Description Total number of register bytes in the application program.

Number of IO allocation errors: <number>

Description Number of unallocated IO, or IO whose allocation is not complete.

Number of markers: <number>

Description Total number of markers used in the application program.

Number of system allocation errors: <number>

Description Number of registers, markers, counters or timers that have been allocated more than once.

O

One or more FLDs missing. First FLD: <number>

Description Not all FLD files were found in the project folder, although they are specified in the databases.

Solution Use the Application Editor to delete the FLDs from the database. The displayed FLD number is the first FLD that is found missing and will be the FLD with the highest number.

Overlapping SOE ID range detected between controller <Controller_Name_x> and <Controller_Name_y>

Description The plant contains two or more SM Controllers with overlapping SOE ID ranges.

Solution Use the Network Configurator to configure disjunct ranges.

P

Point not found in database: <type> <tag number>

Description The point found in the FLD is not found in the data file. The Application Compiler will try to regenerate the point. The result of that action is logged.

Solution Use the Application Editor to enter the required data. The point will then be placed in the database. If the point is a repeated input, you must first place the actual input. It is possible that the data was deleted via the Point Configurator. Use this option to (re-)enter the missing point.

Point not linked to current application: <type> <tag number> (<linked appl. name>)

| | |
|---|--|
| Description | The specified point does not exist in the other application database, or is linked to another Safety Manager. For example, TEST_1 in the current application is a digital input called Link1, which is linked to TEST_2. There is a digital output Link1 in application TEST_2, but this point is linked to system 3. |
| Solution | Rebuild the database. |
| Power-on value out of range. <type> <tag number> | |
| Description | The power-on value of the point is invalid. |
| Solution | Use the Point Configurator to change the power-on value. |
| Program aborted. Application configuration not defined. | |
| Description | Before using the Application Compiler, the Safety Manager Application configuration should be known. |
| Solution | Use the configuration tools to define the Safety Manager application. |
| Program interrupted manually. | |
| Description | The compilation process was interrupted because the <Esc> key was pressed. |

R

Reference to non-existing FLD: <FLD>

| | |
|---|---|
| Description | The specified FLD is undefined or cannot be found on disk. |
| Solution | Use the Application Editor to delete the reference. |
| Register allocation error: <type> <tag number> Byte number: <byte no.> | |
| Description | The point in the register area has the specified address, which is already (partially) used by one or more other points in the register area. |
| Solution | Use the Point Configurator to check the addresses of all points or rebuild using the Database Rebuilder. |
| Reset signal must be connected: <type> <tag number> | |
| Description | A memorize timer must always have a reset signal because you cannot get it low after you started it. |
| Solution | Make sure the memorize timer has a reset signal. |

S

Safety Manager system out of memory for this type of point: <type> <Point no.>

| | |
|-------------|---|
| Description | The Application Compiler cannot place a compiler register or compiler marker in the point database. |
|-------------|---|

Solution 1 It is possible that new space will be created after the compilation is complete. Therefore, recompile the whole set. Erase any unused points (FLD number is 0). Change your design so as to decrease the number of required markers and/or registers.

Solution 2 Reduce the number of bytes reserved to communicate markers and registers to external devices. (Excluding SafeNet connections.) This will free up space for application markers and registers.

Set and value signals must both be connected or not connected: <type> <tag number>

Description If you have a set function, you need a value to be loaded into the counter. If you do not have a set function, no value is needed.

Solution Make sure a value is loaded into the counter.

Set, count-up or count-down signal must be connected: <type> <tag number>

Description You must connect one of these functions to the counter for it to be of any use.

Solution Make sure one of the specified functions is connected to the counter.

Set signal must be connected.

Description The set signal of a timer has not been connected.

Solution Use the Application Editor to create a connection.

Signal type does not match number of bits: <type> <tag number>

Description The signal type does not have the number of bits that it should have.

Solution Use the Point Configurator and change signal type of the point.

T

Timeout inconsistency detected.

Description This warning may be generated in case of Safety Manager communication on low baud rates. In order to guarantee correct handling, the configured Safety Manager communication time-out should be identical for all applications in a network. Any mismatches are reported as a warning, with the affected system(s) specified.

Solution Make sure that the Safety Manager communication time-out for all connected systems in a network is identical.

Timer allocation error <type> <tag number> Byte number: <byte>

Description The timer has the specified address, which is already used by one or more other timers.

Solution Use the Database Rebuilder to check the addresses of all points.

Time zone configuration can not be retrieved from the Windows registry.

| | |
|--|---|
| Description | The specifications for the timezone configured for the Plant, can not be retrieved from the Windows registry. The Windows registry could be corrupted or registry data may have been deleted inadvertently. |
| Solution | Repair the Windows registry or compile the application on a PC with correct timezone specifications. |
| Too many appl. connected for COM channel (COM module, Chan): <seq.> <chan.> | |
| Description | The identified channel from the communication module has been specified as an external point-to-point SafeNet protocol, but too many external applications have been specified. |
| Solution | Use the Network Configurator to specify only one communication link, or change the point-to-point link to a multidrop link. |
| Too many masters specified for (COM, Ch): <COM module>, <channel> | |
| Description | The specified communication channel has been linked to several applications, but too many masters have been specified. |
| Solution | Use the Network Configurator to remove master applications from the specified channel. |
| Too many signal lines connected to one symbol: Node (x, y) | |
| Description | The number of signal lines to one symbol is limited by the Application Compiler. |
| Solution | Change the functional logic diagrams by splitting the symbol into two symbols. |
| Top and bottom values are identical: <type> <tag number> | |
| Description | The range of the specified point has not been defined. |
| Solution | Use the Point Configurator to specify the top and bottom value of the point. |
| Total block size for the DCS buffer is too large. | |
| Description | The total size of marker and register (input and output) bytes on all logical connections of the SM Controller -SafeNet excluded, is larger than the maximum allowed of 8696. |
| Solution | Reconfigure sizes in Network Configurator. |
| Total block size for the SafeNet buffer is too large. | |
| Description | The total size of marker and register (input and output) bytes on all logical SafeNet connections, is larger than the maximum allowed of 4000. |
| Solution | Reconfigure sizes in Network Configurator. |
| Total marker block size for the DCS buffer is invalid. | |
| Description | The total size of marker (input and output) bytes on all logical connections of the SM Controller -SafeNet excluded, is larger than the maximum allowed of 508. |
| Solution | Reconfigure sizes in Network Configurator. |
| Total marker block size for the SafeNet buffer is invalid. | |

Description The total size of marker (input and output) bytes on all logical SafeNet connections of the SM Controller, is larger than the maximum allowed of 508.

Solution Reconfigure sizes in Network Configurator.

Total number of errors detected during compilation: <number>

Description This is the total number of errors that were found during compilation.

Total number of warnings generated during compilation: <number>

Description This is the total number of warnings that were generated during compilation.

Total register block size for the DCS buffer is invalid.

Description The total size of register (input and output) bytes on all logical connections of the SM Controller -SafeNet excluded, is larger than the maximum allowed of 8188.

Solution Reconfigure sizes in Network Configurator.

Total register block size for the SafeNet buffer is invalid.

Description The total size of register (input and output) bytes on all logical SafeNet connections of the SM Controller, is larger than the maximum allowed of 4000.

Solution Reconfigure sizes in Network Configurator.

U

Unable to create Safety Manager file backup

Description Safety Builder was not able to create a backup of the existing Safety Manager file.

Solution Remove old Safety Manager file.

Unable to create object

Description internal error

Solution contact Honeywell SMS

Unable to create user interface of

Description internal error

Solution contact Honeywell SMS

Undefined FLD reference: <type> <tag number>

Description A reference was found to FLD 0 or from FLD 0, which has not been defined.

Solution Use the Application Editor to define the FLD reference.

Unexpected IO module at (chassis, slot, channel): (<chassis>, <pos.>, <chan.>) <type> <tag number>

| | |
|--|--|
| Description | The specified point has been allocated to an invalid module type (e.g. a digital input point has been allocated to an analog output module). |
| Solution | Use the Point Configurator to reallocate the point. |
| Unnecessary signal conversion. Node (x,y) | |
| Description | A signal conversion is performed but the source signal is identical to the destination signal. |
| Solution | Use the Application Editor to remove this signal conversion. |

V

Value (or base) in FLD and point data file are not equal: <type> <tag number>

| | |
|-------------|--|
| Description | The value of the point (timer or counter) has been changed in the database but not in the FLD. |
| Solution | Use the Application Editor to change the point. |

Value signal must be connected.

| | |
|-------------|---|
| Description | A binary input for this type of timers must be connected. |
| Solution | Use the Application Editor to create a connection. |

Value signal must not be connected.

| | |
|-------------|--|
| Description | A binary input for this type of timers may not be connected. |
| Solution | Use the Application Editor to remove the binary input. |

W

Wrong number of input signals: Node (x, y)

| | |
|-------------|--|
| Description | The number of signals at the input side of the symbol does not match the expected number of signals. |
| Solution | Run the Application Editor to change the number. |

List of abbreviations

| | |
|---------|--|
| AI | Analog Input |
| AO | Analog Output |
| ASM | Abnormal Situation Management |
| ATEX | Explosive Atmosphere (in French: “ AT mospheres EX plosibles”) |
| BKM | Battery and Key switch Module |
| BMS | Burner Management System |
| CEE | Control Execution Environment |
| CP | Control Processor |
| DCF | Digital Coded Frequency |
| DCS | Distributed Control System |
| DI | Digital Input |
| DO | Digital Output |
| DTI | Diagnostic Test Interval |
| E/E/PES | Electrical/Electronic/Programmable Electronic System |
| EMC | Electromagnetic Compatibility |
| ESD | <ul style="list-style-type: none"> • Electrostatic Discharge • Emergency ShutDown system |
| EUC | Equipment Under Control |
| EUT | Equipment Under Test |
| F&G | Fire and Gas |
| FB | Function Block |
| FGS | Fire and Gas System |
| FLD | Functional Logic Diagram |
| FSC | <ul style="list-style-type: none"> • Fail Safe Communication • Fail Safe Controller |
| FTA | Field Termination Assembly |
| FTE | Fault Tolerant Ethernet |
| GPS | Global Positioning System |
| HIPS | High-Integrity Protection Systems |
| HMI | Human Machine Interface |
| HSE | High Speed Ethernet |
| IO | Input/Output |

List of abbreviations

| | |
|-------|--|
| IP | <ul style="list-style-type: none">• Internet Protocol• Ingress Protection |
| IS | Intrinsically Safe |
| LAN | Local Area Network |
| LED | Light-Emitting Diode |
| MAC | Media Access Control |
| MAP | Manufacturing Automation Protocol |
| MOS | Maintenance Override Switch |
| MTBF | Mean Time Between Failure |
| MTTF | Mean Time To Failure |
| MTTR | Mean Time To Repair |
| NTP | Network Time Protocol |
| OLE | Object Linking and Embedding |
| OPC | Object linking and embedding for Process Control |
| OS | Operating System |
| P&ID | Piping and Instrumentation Diagram |
| PCDI | Peer Control Data Interface |
| PE | Protective Earth |
| PES | Programmable Electronic System |
| PFD | Probability of Failure on Demand |
| PKS | Process Knowledge System |
| PLC | Programmable Logic Controller |
| PST | Process Safety Time |
| PSU | Power Supply Unit |
| PTP | Precision Time Protocol |
| PUC | Process Under Control |
| PV | Process Value |
| QMR | Quadruple Modular Redundant |
| QPP | Quad Processor Pack |
| RFI | Radio Frequency Interference |
| SCADA | Supervisory Control And Data Acquisition |
| SIC | System Interconnection Cable |
| SIF | Safety Instrumented Function |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System |

| | |
|------|---|
| SMOD | Secondary Means Of De-energization |
| SOE | Sequence Of Events |
| SRS | Safety-Related System |
| STP | Shielded Twisted Pair |
| USI | Universal Safety Interface |
| UTP | Unshielded Twisted Pair |
| UTC | Coordinated Universal Time (Universal Time Coordinated) |
| WAN | Wide Area Network |

Safety Manager Glossary

A

Alarm

An automatic signal that serves as a warning of an event or danger.

Application

The definition of the EUC-dependent function for Safety Manager.

Application Compiler

A tool of the Safety Builder used to create a controller file.

Application Editor

A tool of the Safety Builder used to create or edit functional logic diagrams.

Application value

The value of a process point as provided to, or calculated by, the application software.

Application Viewer

A tool of the Safety Builder used to view functional logic diagrams on-line.

ATEX Directive

A directive which describes equipment and protective systems intended for use in potentially explosive atmospheres.

Safety Manager ATEX modules can be used for connection to hazardous locations in compliance with EN 60079-15:2005 (zone 2, sub groups IIA, IIB and IIC).

For more information see the *Safety Manager TUV EExn Approval Manual* (PM.MAN.8183)

Availability

- The ratio of system up time to total operating time.
- The ability of an item to perform its designated function when required for use.

B

Battery and Key switch Module (BKM)

A module in the SM Controller used to:

- Supply battery power to the system memory (RAM) and the real time clock of the Control Processor modules, in case of power outage.
- Enable or disable forces, by turning the Force key switch. When enabled, forcing of certain input and output signals is allowed. When disabled, all forces are removed.
- Provide a fault reset, by turning the Reset key switch. See Fault reset.



Warning

Turning the Reset key switch during an On-Line Modification procedure may cause the Control Processors to swap status.

C

Communication module

See: Universal Safety Interface (USI)

Communication redundancy fail-over

The automated capability of a device to switch over to a redundant or dormant communication path upon the failure or abnormal termination of the active path.

Communication time-out

An error caused by an unacceptable large time interval during which there was no communication.

Control Processor (CP)

Core component of the SM Controller consisting of: Power Supply Unit (PSU), Quadruple Processor Pack (QPP) and 1 or 2 communication modules (USI).

Control Processor states

A Control Processor (CP) can have many states. For fault detection and response only the following states are relevant.

- `running` (without faults); CP is fully functional and runs the application.
- `running with faults`; CP runs the application but lacks certain functions
- `halted`

The applicable CP state can be read from the User Interface Display located on each Control Processor and from the diagnostic screens available on Experion™ and Safety Stations.

Controller chassis

19" chassis to slot the BKM and Control Processor modules.

Controller Management

A tool of the Safety Builder used to perform the following functions:

- Load controller.
- View system status.
- Retrieve controller and application files.

Coordinated Universal Time (UTC)

Also referred to as “Universal Time Coordinated” and “Zulu time”.

An atomic realization of Universal Time (UT) or Greenwich Mean Time (GMT), the astronomical basis for civil time. Time zones around the world are expressed as positive and negative offsets from UT. UTC differs by an integral number of seconds from atomic time and a fractional number of seconds from UT1.

Cycle time

The time period needed to execute the application software once.

D

Dangerous failure

Failure which has the potential to put the safety-related system in a hazardous or fail-to-function state.



Note

Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

Database Rebuilder

Repair function for the information storage for Safety Builder created databases.

Deutsches Institut für Normung (DIN)

German Institute for Standards, which determines the standards for electrical and other equipment in Germany.

Diagnostic Test Interval (DTI)

The time period used by Safety Manager to cyclically locate and isolate safety related faults within on-line system components that could otherwise cause a hazardous situation.

With Safety Manager, the default DTI is set at 3 seconds. This setting needs to be verified for each process.

See also “Process safety time (PST)” on page 534.

Distributed Control System (DCS)

System designed to control industrial processes. A DCS receives the measured values of the process instrumentation, e.g. flow, pressure, temperature. It controls the process via analog control equipment such as control valves. In addition, a DCS may receive many digital signals for alarm and management purposes.

Dual Modular Redundant (DMR)

Safety configuration providing 1oo2 configuration. The DMR technology is used in the architecture of a non redundant QPP where on-board 1oo2D voting is based on dual-processor technology.

DMR is characterized by a high level of diagnostics and fault coverage.

E

Electrical/Electronic/Programmable Electronic (E/E/PE) device

A device based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology.



Note

This term is intended to cover any and all devices operating on electrical principles and would include:

- electro-mechanical devices (“electrical”);
 - solid state non-programmable electronic devices (“electronic”);
 - electronic devices based on computer technology (“programmable electronic”).
-

Electrical/Electronic/Programmable Electronic system (E/E/PES)

A system based on one or more E/E/PE devices, connected to (and including) input devices (e.g. sensors) and/or output devices/final elements (e.g. actuators), for the purpose of control, protection or monitoring.

See also: “Programmable electronic system (PES)” on page 534.

Electromagnetic Compatibility (EMC)

The ability of a device, equipment or system to function satisfactory in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment.

Electrostatic discharge (ESD)

The transfer of electrostatic charge between bodies of different electrostatic potential, which may cause damage to system components.

Emergency Shutdown (ESD)

Manual or automatic turning off or closing down of process equipment in case of anomalous conditions in order to prevent damage to the system or process.

EUC risk

Risk arising from the EUC or its interaction with the EUC control system.

See also “Equipment Under Control (EUC)” on page 523.

Equipment Under Control (EUC)

Equipment/machinery/apparatus/Plant used for manufacturing, process, transportation, medical or other activities for which designated safety-related systems could be used to:

- prevent hazardous events associated with the EUC from taking place; or,
- mitigate the effects of the hazardous events.

Error

Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition.

Ethernet

A local area network specification developed by Xerox in 1976. The specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers of the network. It uses CSMA/CD to handle simultaneous transmissions and is the most popular LAN Technology in use today.

See also: Local Area Network (LAN).

Event

- Occurrence of some programmed action within a process which can affect another process.
- Asynchronous occurrence that is detected by the control system, time and other information is recorded, e.g. process alarm.

Experion PKS

Honeywell Process Knowledge System™ for process, business and asset management.

Experion Station

Windows based station for viewing process schematics and interactions with the system. This station provides comprehensive alarm and event detection, management, reporting facilities, and history collection along with the capability of custom process graphics.

Event collection & management system

A device used to collect, log and manage sequence of events (SOE) data.

See also Sequence Of Events (SOE).

External device

A generic term for a system the SM Controller is communicating with. This may be an Experion server, a Modbus device, a Safety Station or even another SM Controller.

External risk reduction measures

Physical measures taken externally to safety-related systems to reduce or mitigate the risks. Examples would include a drain system, fire wall, etc.

F

Fail-over

See “Communication redundancy fail-over” on page 520.

Failure

The termination of the ability of a functional unit to perform a required function.



Note

- The definition in IEC 191-04-01 is the same, with additional notes.
 - See figure in “Functional Safety” for the relationship between faults and failures, both in IEC 61508 and IEC 191.
 - Performance of required functions necessarily excludes certain behavior, and some functions may be specified in terms of behavior to be avoided. The occurrence of such behavior is a failure.
 - Failures are either random (in hardware) or systematic (in hardware or software).
-

Fault

Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.

**Note**

IEV 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources.

Fault reaction

The response to faults in the Controller, application and/or IO.

- The fault reaction towards Controller and/or application faults is fixed.
- The fault reaction towards IO faults can be configured on a module level and should be customized to the application for which Safety Manager is used.

See also “IO states” on page 530.

Fault reset

An action that clears the fault database and attempts a restart of tripped or halted components of the system.

Fault Tolerant Ethernet (FTE)

An Ethernet based control network of Experion PKS.

FC

Prefix used to identify conformal-coated module from non conformal coated modules. See also: FS.

- FC-SDI-1624 is a safe digital input module with conformal coating
- FS-SDI-1624 is a safe digital input module without conformal coating

Field Termination Assembly (FTA)

Assembly to connect field wiring to the SM IO modules.

Field value

The value of a process point as present at the interface of the system with the EUC.

Fieldbus

Wiring solution and communication protocol in which multiple sensors and actuators are connected to a DCS or SIS, using a single cable.

Fire and Gas system

Independent protective system which continuously monitors certain process points (e.g. combustible gas levels) and environmental points (e.g. heat, smoke, temperature and toxic gas levels). If any of these points exceed a predetermined level, the system will raise an alarm and take automatic action to close operating valves and damper doors, activate extinguishers, cut off electrical power and vent dangerous gases.

Force

A signal override of some sort that is applied on a system level.

A force applied to an input affects the input application state as it overrides the actual field value and diagnostic state of the forced input.

A force applied to an output affects the output field state as it overrides the application value or diagnostic value with the forced value.



Caution

Forcing introduces a potentially dangerous situation as the corresponding point could go unnoticed to the unsafe state while the force is active.

FS

Prefix used to identify non conformal-coated module from conformal coated modules. See also: FC.

- FS-SDI-1624 is a safe digital input module without conformal coating
- FC-SDI-1624 is a safe digital input module with conformal coating

Function block

Element in a functional logic diagram (FLD) which performs a user defined logic function. Function blocks are designed to implement & re-use complex functions via a single (user defined) element.

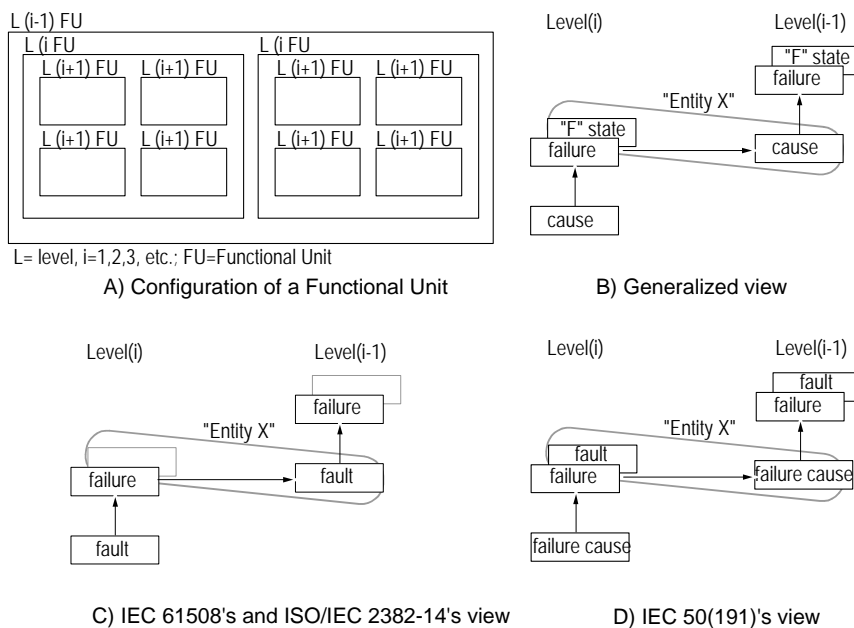
Functional Logic Diagram (FLD)

Diagrammatic representation of the application (conform the IEC 61131-3 standard) which is used to program Safety Manager. FLDs are directly translated into code that can be executed by Safety Manager, thus eliminating the need for manual programming. See also: Application Editor.

Functional safety

Part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

Figure 94 Failure model



Notes for Figure 94 on page 527

- As shown in A), a functional unit can be viewed as a hierarchical composition of multiple levels, each of which can in turn be called a functional unit. In level (i), a "cause" may manifest itself as an error (a deviation from the correct value or state) within this level (i) functional unit, and, if not corrected or circumvented, may cause a failure of this functional unit, as a result of which it falls into an "F" state where it is no longer able to perform a required function (see B)). This "F" state of the level (i) functional unit may in turn manifest itself as an error in the level (i-1) functional unit and, if not corrected or circumvented, may cause a failure of this level (i-1) functional unit.
- In this cause and effect chain the same thing ("Entity X") can be viewed as a state ("F" state) of the level (i) functional unit into which it has fallen as a result of its failure, and also as the cause of the level (i-1) functional unit. This "Entity X" combines the concept of "fault" in IEC 61508 and ISO/IEC 2382-14, which emphasizes its cause aspect as illustrated in C), and that of "fault" in IEC 50(191), which emphasizes its state aspect as illustrated in D). The "F" state is called fault in IEC 50(191), whereas it is not defined in IEC 61508 and ISO/IEC 2382-14.
- In some cases, a failure may be caused by an external event such as lightning or electrostatic noise, rather than by an internal fault. Likewise, a fault (in both vocabularies) may exist without a prior failure. An example of such a fault is a design fault.

Functional safety assessment

Investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities.

H

Hardware Configurator

A tool of the Safety Builder used to configure the hardware of Safety Manager.

Hardware safety integrity

Part of the safety integrity of the Safety Instrumented Systems (SIS) relating to random hardware failures in a dangerous mode of failure.



Note

The term relates to failures in a dangerous mode. That is, those failures of a safety-related system that would impair its safety integrity. The two parameters that are relevant in this context are the overall dangerous failure rate and the probability of failure to operate on demand. The former reliability parameter is used when it is necessary to maintain continuous control in order to maintain safety, the latter reliability parameter is used in the context of safety-related protection systems.

Hazard

A physical situation with a potential for human injury.



Note

The term includes danger to persons arising within a short time scale (e.g. fire and explosion) and also those that have a long-term effect on a persons health (e.g. release of a toxic substance).

High voltage

A voltage of 30VAC, 40VDC or above.

Human error

Mistake.

Human action or inaction that produces an unintended result.

I

IEC 61131-3

Part of the international standard IEC 61131, which provides a complete collection of standards on programmable controllers and their associated peripherals.

The IEC 61131-3 specifies the syntax and semantics of programming languages for programmable controllers as defined in part 1 of IEC 61131 (FLD symbols).

IEC 61508

International IEC standard on functional safety entitled “Functional safety: safety-related systems”, which sets out a generic approach for all electrically based systems that are used to perform safety functions. A major objective of this international standard is to facilitate the development of application sector standards.

Institute of Electrical and Electronic Engineers (IEEE)

An American professional organization of scientists and engineers whose purpose is the advancement of electrical engineering, electronics and allied branches of engineering and science. It also acts as a standardization body.

International Electrotechnical Commission (IEC)

An international standards development and certification group in the area of electronics and electrical engineering, including industrial process measurement, control and safety.

Interval time between faults

See: Repair timer.

IO bus

A bus-structure within Safety Manager that interconnects the Control Processor with the IO.

IO bus driver

Part of the Quad Processor Pack that controls the IO bus.

IO chassis

19” chassis to slot the (redundant) IO extender(s) and SM IO modules.

IO database

Database in which input, output and configuration data is stored.

IO extender

Module which controls the IO bus of the IO chassis. A maximum of ten IO extender modules can be connected to one IO bus.

IO module

Module which handles input or output functions of Safety Manager. IO modules can be digital or analog.

IO states

From a SIS point of view, IO can have either the healthy state, the de-energized state or the fault reaction state.

- When healthy, the IO is active and has the application value or a forced value applied.
- When de-energized, the IO is de-activated (as if no power was supplied).
- When the fault reaction state is applied, the IO responds conform a predefined fault condition (fault reaction).

L

Local Area Network (LAN)

A general term to refer to the network and its components that are local to a particular set of devices.

See also: Wide area network (WAN).

M

Maintenance override

A function, which allows the user to apply an application value to an input independent of the input channel scan value.

Maintenance Override Switch (MOS)

Switch used to file a request for a maintenance override. Acknowledgement is decided by the application program. An acknowledged maintenance override allows maintenance to be performed on field sensors or field inputs without causing the safety system to trip the process.

Master-clock source

The source that is responsible for the time synchronization between a group of systems or within a network.

Mean Time Between Failure (MTBF)

- For a stated period in the life of a functional unit, the mean value of the length of time between consecutive failures under stated conditions.
- The expected or observed time between consecutive failures in a system or component.

MTBF is used for items which involve repair.

See also: Mean Time To Repair (MTTR), Mean Time To Failure (MTTF).

Mean Time To Failure (MTTF)

The average time the system or component of the system works without failing.

MTTF is used for items with no repair.

See also: Mean Time To Repair (MTTR), Mean Time Between Failure (MTBF).

Mean Time To Repair (MTTR)

The mean time to repair a safety-related system, or part thereof. This time is measured from the time the failure occurs to the time the repair is completed.

Media Access Control (MAC)

The lower sublayer of the data link layer (Layer 2) unique to each IEEE 802 local area network. MAC provides a mechanism by which users access (share) the network.

Modbus

A communications protocol, based on master/slave or client/server architecture, originally designed by Modicon for use with PLC and SCADA systems. It has become a de facto standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices.

Mode of operation

Way in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it in relation to the proof check frequency, which may be either:

- **Low demand mode** - where the frequency of demands for operation made on a safety-related system is not significantly greater than the proof check frequency; or
- **High demand or continuous mode** - where the frequency of demands for operation made on a safety-related system is significantly greater than the proof check frequency.



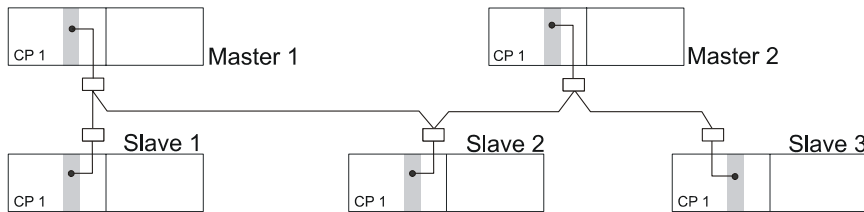
Note

Typically for low demand mode, the frequency of demands on the safety-related system is the same order of magnitude as the proof test frequency (i.e. months to years where the proof test interval is a year). While typically for high demand or continuous mode, the frequency of demands on the safety-related system is hundreds of times the proof test frequency (i.e. minutes to hours where the proof test interval is a month).

Multidrop link

A multidrop link is a physical link that interconnects multiple systems (see Figure Figure 95 on page 532).

Figure 95 Multidrop link



N

Namur

A 2-wire proximity switch operating at a working voltage of 8.2 V and an operating current of 8mA max (CENELEC Standard). Because of the small amount of energy needed to operate NAMUR sensors, they can be used in intrinsically safe applications.



Note

Special switching amplifiers or dedicated input modules, like the SDIL-1624, are required to read the status of NAMUR proximity switches.

Network Configurator

A tool of the Safety Builder used to configure the communication architecture.

Network Time Protocol (NTP)

See “Time protocol” on page 544.

Node

Hardware entity connected to a network.

O

Object linking and embedding for Process Control (OPC)

Technology developed originally by Microsoft, now being standardized. Microsoft technology for application interoperability. Object Linking and Embedding (OLE) is a set of services that provides a powerful means to create documents consisting of multiple sources of information from different applications. Objects can be almost any type of information, including text, bitmap images, vector graphics, voice, or video clips.

Off-line

A system is said to be “off-line” when it is not in active control of equipment or a process.

A process or equipment is said to be “off-line” when it is in shut-down.

On-line

A system is said to be “on-line” when it is in active control of equipment or a process.

A process or equipment is said to be “on-line” when it is operating.

Operating temperature

The temperature a system is operating on. The operating temperature is measured in the CP chassis at the QPP module.

Operational state

The values of an application point during normal process operation.

P

Peer Control Data Interface (PCDI)

A Honeywell licensed communication interface for non-safe peer-to-peer data communication between (Experion) CEE controllers and SM Controllers.

Peer-to-peer

A logical connection between two points.

Plant

A component in Safety Builder which contains devices, controllers as well as physical and logical communication configurations used to interconnect these devices and controllers.

Point

A data structure in the IO database, usually containing information about a field entity. A point can contain one or more parameters. Safety Manager uses different point types to represent a range of different field values.

Point Configurator

A tool of the Safety Builder used to create and modify points of a SM Controller.

Point Viewer

A tool of the Safety Builder used to view points with dynamic update of states and values.

Power Supply Unit (PSU)

Separate module which supplies electrical power to the SM Controller.

Precision Time Protocol (PTP)

See “Time protocol” on page 544

Probability of Failure on Demand (PFD)

A value that indicates the probability of a system failing to respond to a demand. PFD equals 1 minus Safety Availability. (ISA, S84.01, 1996)

Process safety time (PST)

The time a process can be left running uncontrolled without losing the ability to regain control.

See also Diagnostic Test Interval (DTI).

Process states

A process can have many states. Related to fault detection and response in the safety loop of a process, the following process states are described:

- running without detected faults
- running with detected faults
- halted

Process value

An amount, expressed in engineering units, that represents the value of a process variable, e.g. a temperature, a pressure or a flow.

Programmable electronic system (PES)

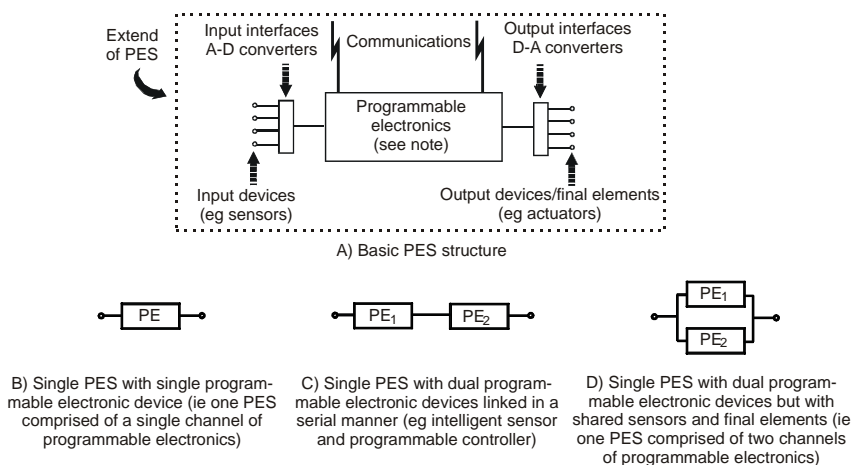
System for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices (see Figure 96 on page 535).



Note

The structure of a PES is shown in Programmable electronic system (PES): structure and terminology A). Programmable electronic system (PES): structure and terminology B) illustrates the way in which a PES is represented in IEC 61508, with the programmable electronics shown as a unit distinct from sensors and actuators on the EUC and their interfaces, but the programmable electronics could exist at several places in the PES. Programmable electronic system (PES): structure and terminology C) illustrates a PES with two discrete units of programmable electronics. Programmable electronic system (PES): structure and terminology D) illustrates a PES with dual programmable electronics (i.e. two channel), but with a single sensor and a single actuator.

Figure 96 Programmable electronic system (PES): structure and terminology



Q

Quad Processor Pack (QPP)

The main processing module of the SM Controller.

Quadruple Modular Redundant (QMR)

Safety configuration providing a 2oo4D configuration. The QMR technology is used in the architecture of a redundant QPP where on-board 1oo2D voting (see Dual Modular Redundant (DMR)) is combined with 1oo2D voting between the two QPPs.

Voting takes place on two levels: First on a module level and secondly between the Control Processors.

QMR is characterized by a high level of diagnostics, fault coverage and fault tolerance.

R

Redundancy

- In an item, the existence of more than one means of performing a required function.
- Use of duplicate (or triple or quadruple) modules or devices to minimize the chance that a failure might disable an entire system.

Repair time

The time allowed to keep a Safety Instrumented System (SIS) running with a fault present that “may affect safety upon accumulation of multiple faults”. Repair time is introduced to extend the SIS up-time for a limited time frame, allowing system repair.

Repair timer

A configurable count-down timer triggered upon detection of a fault that minimizes the safety availability of the system.

The default repair window is 200 hours, which is more than sufficient if spare parts are available. The repair timer can be deactivated.

Each Control Processor has its own repair timer. Once running, a repair timer shows the remaining time to repair the fault that triggered the repair timer in the Control Processor (200 hours default). If the fault is not repaired within the repair time the Control Processor containing the fault halts.

A repair timer protects the system from certain fault accumulations that may affect the safety of Safety Manager. The timer only starts on detection of:

- faults on output modules with fault reaction set to `Low`
- faults detected with non-redundant IO bus extenders.

Reset

See: Fault reset.

Risk

Combination of the probability of occurrence of harm and the severity of that harm.

Router

A network device which forwards packets (messages or fragments of messages) between networks.

The forwarding decision is based on network layer information and routing tables, often constructed by routing protocols.

S

Safe

A design property of an item in which the specified failure mode is predominantly in a safe direction.

Safe failure

Failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state.



Note

Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a safe hardware failure is less likely to result in an erroneous shutdown.

SafeNet

A SIL3 network protocol used by Safety Manager for i.e. safe data exchange between Safety Managers.

Safety

Freedom from unacceptable risk.

Safety Availability

The fraction of time (%) that a safety system is able to perform its designated safety service when the process is operating. See also Probability of Failure on Demand (PFD).

Safety Builder

- Station software used to configure, design, validate, log and monitor a Safety Manager project.
- Protocol used by Safety Manager to communicate with Safety Stations.

Safety Instrumented Function (SIF)

A Safety Instrumented Function (SIF) is an isolated function, initially designed to protect “life and limb” against a specific hazard. A more popular term for SIF is safety loop. Each SIF operates on its own Safety Integrity Level.

See also Safety instrumented System (SIS) and Safety integrity level (SIL).

Safety instrumented System (SIS)

A Safety Instrumented System (SIS) is a system that executes one or more SIFs. The various SIFs inside a SIS may each require a different Safety Integrity Level. A SIS should be able to support all SIFs, including the one with the highest SIL level.


See also Safety Instrumented Function (SIF) and Safety integrity level (SIL).

Safety integrity

Probability of a safety-related system to satisfactorily perform the required safety functions under all stated conditions within a stated period of time.

Safety integrity level (SIL)

Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.



Note

- The target failure measures for the safety integrity levels are specified in Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in low demand mode of operation and Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in high demand or continuous mode of operation.

Table 47 Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in low demand mode of operation

| Safety integrity level | Low demand mode of operation (average probability of failure to perform its design function on demand) |
|---|---|
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ |
| NOTE: see notes below for details on interpreting this table. | |

Table 48 Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in high demand or continuous mode of operation

| Safety integrity level | High demand or continuous mode of operation (probability of a dangerous failure per hour) |
|---|---|
| 4 | $\geq 10^{-9}$ to $< 10^{-8}$ |
| 3 | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-6}$ to $< 10^{-5}$ |
| NOTE: see notes below for details on interpreting this table. | |



Note

1. The parameter in Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in high demand or continuous mode of operation, probability of a dangerous failure per hour, is sometimes referred to as the frequency of dangerous failures, or dangerous failure rate, in units of dangerous failures per hour.
2. This document sets a lower limit on the target failure measures, in a dangerous mode of failure, than can be claimed. These are specified as the lower limits for safety integrity level 4 (that is an average probability of failure of 10^{-5} to perform its design function on demand, or a probability of a dangerous failure of 10^{-9} per hour). It may be possible to achieve designs of safety-related systems with lower values for the target failure measures for non-complex systems, but it is considered that the figures in the table represent the limit of what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.
3. The target failure measures that can be claimed when two or more E/E/PE safety-related systems are used may be better than those indicated in Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in low demand mode of operation and Safety integrity levels: target failure measures for a safety function, allocated to the Safety Instrumented System operating in high demand or continuous mode of operation providing that adequate levels of independence are achieved.
4. It is important to note that the failure measures for safety integrity levels 1, 2, 3 and 4 are target failure measures. It is accepted that only with respect to the hardware safety integrity will it be possible to quantify and apply reliability prediction techniques in assessing whether the target failure measures have been met. Qualitative techniques and judgements have to be made with respect to the precautions necessary to meet the target failure measures with respect to the systematic safety integrity.
5. The safety integrity requirements for each safety function shall be qualified to indicate whether each target safety integrity parameter is either:
 - the average probability of failure to perform its design function on demand (for a low demand mode of operation); or
 - the probability of a dangerous failure per hour (for a high demand or continuous mode of operation).

Safety life cycle

Necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are no longer available for use.

Safety Manager

A safety solution to protect the integrity of the process. Safety Manager includes the following components:

- Safety Manager
- Safety Station

For details see the *Overview Guide*.

Safety related

A flag to indicate that a signal is used for a safe function.

See also Safe and Safety-related system.

Safety-related system

Designated system that both:

- implements the required safety functions necessary to achieve or maintain a safe state for the EUC, and
- is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions.

**Note**

1. The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the external risk reduction facilities, the necessary risk reduction in order to meet the required tolerable risk.
2. The safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on receipt of commands. The failure of a safety-related system would be included in the events leading to the identified hazard or hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to achieve, in their own right, the required tolerable risk. Safety-related systems can broadly be divided into safety-related control systems and safety-related protection systems, and have two modes of operation.
3. Safety-related systems may be an integral part of the EUC control system or may interface with the EUC by sensors and/or actuators. That is, the required safety integrity level may be achieved by implementing the safety functions in the EUC control system (and possibly by additional separate and independent systems as well) or the safety functions may be implemented by separate and independent systems dedicated to safety.
4. A safety-related system may:
 - be designed to prevent the hazardous event (that is if the safety-related systems perform their safety functions then no hazard arises). The key factor here is the ensuring that the safety-related systems perform their functions with the degree of certainty required (for example, for the specified functions, that the average probability of failure should not be greater than 10^{-4} to perform its design function on demand).
 - be designed to mitigate the effects of the hazardous event, thereby reducing the risk by reducing the consequences. As for the first item in this list, the probability of failure on demand for the specified functions (or other appropriate statistical measure) should be met.
 - be designed to achieve a combination of both kinds of systems.
5. A person can be part of a safety-related system. For example, a person could receive information from a programmable electronic device and perform a safety task based on this information, or perform a safety task through a programmable electronic device.
6. The term includes all the hardware, software and supporting services (for example power supplies) necessary to carry out the specified safety function (sensors, other input devices, final elements (actuators) and other output devices are therefore included in the safety-related system).
7. A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable electronic, hydraulic and pneumatic.

Safety Station

Station running Safety Builder and Safety Historian.

Second fault timer

See: Repair timer.

Secondary Means

A means designed to drive towards a safe state in case the primary means is unable or unreliable to do so.

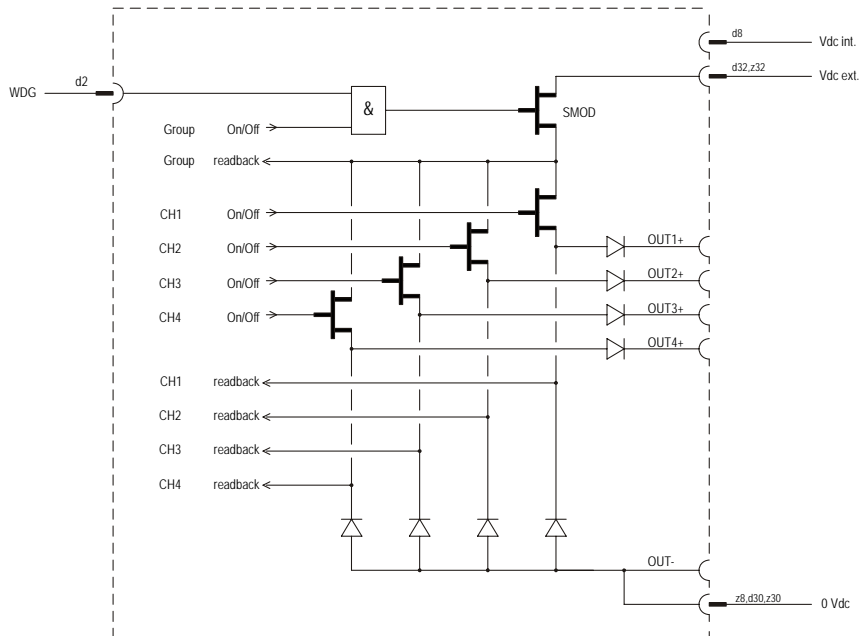
An example of a secondary means is the watchdog: The watchdog is designed to drive the Control Processor and related outputs to a safe state if the Control Processor itself is unable or unreliable to do so.

Secondary Means Of De-energization (SMOD)

A SMOD is a Secondary Means designed to de-energize the output in case the primary means is unable or unreliable to do so.

Figure 97 on page 542 shows an example of a SMOD protecting 4 output channels.

Figure 97 Schematic diagram of a SMOD with 4 channels



Sequence Of Events (SOE)

The function detecting the occurrence of events. See also: SOE Station and Event collection & management system.

Serial communication

Communication that is based on either an RS232, RS422 or RS485 link.

Shutdown

A process by which an operating Plant or system is brought to a non-operational state.

SICC

IO signal wiring using system interconnection cables that hook up the FTA board to the IO.

SICP

IO signal wiring using system interconnection cables that hook up the screw terminals to the IO.

Single fault tolerant

Built-in ability of a system to correctly continue its assigned function in the presence of a single fault in the hardware or software.

Single fault tolerant for safety

Built-in ability of each Safety Manager configuration to continue to maintain safety in the presence of a single fault in the hardware or software.

SM Controller

Assembly of Control Processor, Controller chassis and BKM. A Controller can be redundant or non redundant. A redundant Controller contains two Control Processors. A non redundant Controller contains one Control Processor. Note that IO is not included.

SM IO

A set of IO chassis linked to a Safety Manager Controller.

Safety Manager

An Safety Manager comprises the following subsystems:

- SM Controller
- SM IO
- FTA

For details see the *Overview Guide*.

Storage temperature

The temperature the system can be stored at.

SOE Station

Sequence of events collecting device. Windows-based software tool used to record, view and process sequence of events (SOE) data. SOE data is stored in a database for (re-)use at a later stage.

See also: Event collection & management system and Sequence Of Events (SOE).

Switch

A network device which forwards packets (messages or fragments of messages) by means of packet switching.

The forwarding decision is based on the most expedient route (as determined by some routing algorithm). Not all packets travelling between the same two hosts, even those from a single message, will necessarily follow the same route.

System Interconnection Cable (SIC)

Cables to connect IO modules with FTAs or terminals.

Systematic safety integrity

Part of the safety integrity of safety-related systems relating to systematic failures in a dangerous mode of failure.



Note

Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can).

T

Time protocol

A collective for Internet protocols to provide machine readable date and time:

- The Precision Time Protocol (PTP) is a protocol that allows precise synchronization of networks. It is used in SafeNet where it reaches clock synchronization accuracies of 10ms.
- The Network Time Protocol (NTP) is an older protocol for synchronizing the clocks of computer systems over internet/ethernet. Safety Manager supports NTP3 and NTP4, reaching clock synchronization accuracies of 100ms.

Timestamp

As a verb, the act of putting the current time together with an event. As a noun, the time value held with an event.

Trend

A display defined primarily for presentation of and navigation through historical information.

Trip

An action by which part of an operating Plant or system is brought to a non-operational state.

See also: Shutdown.

Triple Modular Redundant (TMR)

Safety technology which is based on comparison principles and which requires triplicated system components.

U

Universal Safety Interface (USI)

Communication module of the SM Controller.

V

Validation

Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.

Verification

Confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled.



Note

In the context of IEC 61508, verification means the process of demonstrating for each phase of the relevant safety lifecycle (overall, E/E/PES, software), by analysis and/or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

Examples of verification activities would include:

1. Reviews on deliverables (documents from all phases of the safety lifecycle) to ensure compliance with the objectives and requirements of the phase taking into account the specific inputs to that phase.
 2. Design reviews.
 3. Tests performed on the designed products to ensure that they perform according to their specifications.
 4. Integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.
-

Voting configuration

To prevent that a safety-related system remains passive or false signals occur in this system it is possible to use voting. With voting the safety-related system makes a decision based on signals. The usage of more than one signal enhances the safety and reliability of the system.

W

Watchdog

A combination of diagnostics and an output device (typically a switch) the aim of which is to monitor the correct operation of the programmable electronic (PE) devices and takes action upon detection of an incorrect operation.



Note

The watchdog is used to de-energize a group of safety outputs when dangerous failures are detected in order to put the EUC into a safe state. The watchdog is used to increase the on-line diagnostic coverage of the logic system

Wide area network (WAN)

A general term to refer to a piece of a network and its components that are used to inter-connect multiple LANs over a wide area.

Index

A

- access keys 32
- actual diagnostics 248
- actual output status invalid 475, 476, 477
- add
 - cabinet 129, 137
 - chassis 130
 - component 57
 - module 131
- addition gate 358
- alarm markers
 - behavior 386
 - normal state 386
- allocate automatically 161
- allocation
 - communication ~ 403
- analog
 - loop fault 473, 474
- analog input loop fault 473, 474
- analog inputs 348
- analog outputs 349
- AND 353
- ANN 394
- Application Compiler 226
- application configuration has been modified... 481
- application design 8
- Application Editor 178
- application execution time failure 467
- application program corrupted 470
- Application Viewer 261
- Audit Trail 276
- automatic update of diagnostics 275

B

- backup 64
- basic package 10
- basic skills and knowledge 4

- battery
 - check 472
- binary input function blocks 350, 368
- binary inputs 347
- binary off-sheet transfer 352
- binary on-sheet transfer 351
- binary outputs 349
- BKM transport switch off or fuse blown 472
- BKM-0001
 - BKM transport switch off or fuse blown 472
 - Check battery 472
 - force disable fails 472
- boolean input function blocks 350, 368
- boolean off-sheet transfer 351
- boolean on-sheet transfer 351
- bottom scale 400
- buffer inverter 355
- byte 400

C

- C300 306
- cabinet 129
 - add ~ 129, 137
 - delete ~ 130
 - rename ~ 130
- calculation functions 358
- calculation overflow 464
- CEE Controller
 - properties 85
- change password 283
- change symbol 218
- channel 387
- channels 403
- chassis 130, 403
 - add ~ 130
 - delete ~ 131
 - move ~ 131
 - properties 137
- Check battery 472

- Check VDC power supply voltage 464
- clear not successful 481
- clock Source 260
- clock source 83, 85, 86, 88, 89, 105, 530
- collapse nodes 57
- COM 395
- com module inserted 471
- com module removed 471
- communicate 403
- Communication
 - Delay time on ~ link 505
- communication 325
 - ~ link time-out time 325
- communication allocation 403
- communication links 287, 289
 - logical 287
 - redundant 289
 - SafeNet 289
- communication module faulty 471
- communication networks 287, 288, 289
 - logical link 287
 - master/slave 288
 - multidrop link 288
 - redundant link 289
- communication redundancy 106, 289
- communication statistics 256, 257
- communication status 256, 257
- Communication timeout (SafeNet) 510
- compare functions 356
- compile application 226
- component
 - add ~ 57
 - delete ~ 58, 59
 - move ~ 59
 - rename ~ 60
- configuration 274
 - start ~ 56
 - stop ~ 56
- configuration error 480
- connect 246
 - dis~ 247
 - temporary ~ 247
- connection lines 201, 216, 346
- constant
 - boolean 365
 - value 365
- continuous mode of operation 531, 539
- contractor package 10

- Control Processor halt 470
- controller
 - copy ~ 62
 - enable remote load 64
 - migrating ~s 62
 - selecting a ~ 61
 - set ~ loaded 64
- Controller bar 245
- controller file 226
 - load ~ 251
- Controller Management 240
- Controller not loaded 470
- Controller not running or application
 - configuration different from loaded application 481
- copy 32
 - FLD 191
 - symbol 217
- correlation between channels 478
- counters 362
- CP-CP incompatible Point allocation 470
- create
 - FLD 190
- current detected in output loop 478
- customer information 17
- cut 32
- cycle time 324

D

- dangerous failure 521
- data viewing 292
- database
 - point ~ 162
- day-light saving 74, 86, 88, 106
- daylight saving 333, 443, 447
- DCS
 - properties 87
- Delay time on communication link 505
- Delayed ON timer 374
- delete 32
 - cabinet 130
 - chassis 131
 - component 58, 59
 - confirmation 275
 - point 158
 - symbol 218
- demo package 10

- description 394
- diagnostic input 387
- diagnostic inputs 348, 381, 387
- diagnostic messages 461
- diagnostic test interval 110
- diagnostics 248, 292
 - actual output status invalid 475, 476, 477
 - analog input loop fault 473, 474
 - application configuration has been modified... 481
 - application execution time failure 467
 - application program corrupted 470
 - automatic update 275
 - BKM transport switch off or fuse blown 472
 - calculation overflow 464
 - Check battery 472
 - Check VDC power supply voltage 464
 - clear not successful 481
 - com module inserted 471
 - com module removed 471
 - communication module faulty 471
 - configuration error 480
 - Control Processor halt 470
 - Controller not loaded 470
 - Controller not running or application configuration different from loaded application 481
 - correlation between channels 478
 - CP-CP incompatible Point allocation 470
 - current detected in output loop 478
 - divide by zero 465
 - earth fault detected 474
 - embedded software corrupted 470
 - error code not defined 465, 480
 - ESD input activated 465
 - execution time out of range 470
 - external communication failure 465
 - external power down 478
 - external power down channels 1, 2 478
 - external power down channels 1, 2, 3, 4 476
 - external power down channels 3, 4 478
 - external power down channels 5, 6, 7, 8 476
 - external power down complete module 475
 - external power-down 477
 - external power-down complete module 479
 - force disable fails 472
 - force not successful 482
 - functional logic diagrams different (OLM) 466
 - historical 249
 - idle state initiated due to online modification 471
 - illegal argument, e.g. square root of -1 466
 - illegal command 481
 - illegal counter value (0 .. 8191) 466
 - illegal timer value (0 .. 2047) 466
 - incompatible Safety Builder version 466
 - input compare error 473
 - internal power-down 474, 475
 - key switch cycled from RUN to IDLE 471
 - lead breakage 475
 - line monitor circuit faulty 479
 - memory error 471
 - module
 - faulty 472, 473, 474, 475, 476, 477, 478, 479, 480
 - module faulty, voltage monitoring channel 474
 - no connection 481
 - no differences between applications 467
 - open loop or line monitor circuit faulty 479
 - output channel cannot be switched off 476, 477, 478, 479
 - output channel cannot be switched on 479
 - output compare
 - error 476, 477, 478, 479, 480
 - output is incorrectly switched on 479
 - output short circuit 476, 477, 478, 480
 - Point not found 482
 - power supply to field device shorted 467
 - processor module key in IDLE position 467
 - repair timer expired 468
 - repair timer started 468
 - safe state initiated by other CP 468
 - safe state initiated by software assertion 468
 - secondary switch off asserted 469
 - short-circuits 475
 - spurious watchdog interrupt 469
 - temperature pre-alarm 469
 - temperature sensor faulty 471
 - temperature shutdown 469
 - the application can not be viewed... 482
 - timeout while retrieving status of the Controller 482
 - unable to initialize dynamic arrays for point and line data 482
 - unable to initialize the status of FLD 482
 - unable to start Application Viewer 482
 - voltage output short circuit or module faulty 474

digital
 loop fault 475, 479
 Digital I/O allocation error 497
 digital inputs 347
 digital outputs 349
 disconnect 247
 divide by zero 465
 divide gate 359
 dormant communication path 106, 289
 double line 346
 drag symbol 217
 Duplicate references 485

E

earth fault detected 474
 embedded software corrupted 470
 engineering units 401
 equal gate 356
 equation
 ~ approximation 188
 ~ block 184, 188, 368
 ~ file 188
 ~ function 369
 ~ table 212
 ~ table format 211
 creating ~ blocks 210
 Equipment Under Control (EUC) 5, 6
 error 523, 528
 human ~ 528
 error code not defined 465, 480
 errors
 actual output status invalid 475, 476, 477
 analog input loop fault 473, 474
 application configuration has been
 modified... 481
 application execution time failure 467
 application program corrupted 470
 BKM transport switch off or fuse blown 472
 calculation overflow 464
 Check battery 472
 Check VDC power supply voltage 464
 clear not successful 481
 com module inserted 471
 com module removed 471
 communication module faulty 471
 configuration error 480
 Control Processor halt 470
 Controller not loaded 470
 Controller not running or application
 configuration different from loaded
 application 481
 correlation between channels 478
 CP-CP incompatible Point allocation 470
 current detected in output loop 478
 diagnostic messages 461
 divide by zero 465
 earth fault detected 474
 embedded software corrupted 470
 error code not defined 465, 480
 ESD input activated 465
 execution time out of range 470
 external communication failure 465
 external power down 478
 external power down channels 1, 2 478
 external power down channels 1, 2, 3, 4 476
 external power down channels 3, 4 478
 external power down channels 5, 6, 7, 8 476
 external power down complete module 475
 external power-down 477
 external power-down complete module 479
 force disable fails 472
 force not successful 482
 functional logic diagrams different
 (OLM) 466
 idle state initiated due to online
 modification 471
 illegal argument, e.g. square root of -1 466
 illegal command 481
 illegal counter value (0 .. 8191) 466
 illegal timer value (0 .. 2047) 466
 incompatible Safety Builder version 466
 input compare error 473
 internal power-down 474, 475
 key switch cycled from RUN to IDLE 471
 lead breakage 475
 line monitor circuit faulty 479
 memory error 471
 module
 faulty 472, 473, 474, 475, 476, 477, 478, 4
 79, 480
 module faulty, voltage monitoring
 channel 474
 no connection 481
 no differences between applications 467
 open loop or line monitor circuit faulty 479
 output channel cannot be switched
 off 476, 477, 478, 479

- output channel cannot be switched on 479
 - output compare
 - error 476, 477, 478, 479, 480
 - output is incorrectly switched on 479
 - output short circuit 476, 477, 478, 480
 - Point not found 482
 - power supply to field device shorted 467
 - processor module key in IDLE position 467
 - QPP display messages 458
 - repair timer expired 468
 - repair timer started 468
 - safe state initiated by other CP 468
 - safe state initiated by software assertion 468
 - secondary switch off asserted 469
 - short-circuits 475
 - spurious watchdog interrupt 469
 - temperature pre-alarm 469
 - temperature sensor faulty 471
 - temperature shutdown 469
 - the application can not be viewed... 482
 - timeout while retrieving status of the Controller 482
 - unable to initialize dynamic arrays for point and line data 482
 - unable to initialize the status of FLD 482
 - unable to start Application Viewer 482
 - voltage output short circuit or module faulty 474
 - errors (diagnostic messages) 462
 - ESD input activated 465
 - ethernet
 - gateway address 80
 - IP address 80
 - subnet mask 80
 - EUC risk 523
 - events
 - justification 276
 - execution time out of range 470
 - expand nodes 56
 - Experion protocol 292
 - Experion Server 49
 - properties 86
 - Experion server
 - properties 86
 - Explorer bar 30
 - Controller bar 245
 - FLD bar 183, 264
 - exponent gate 361
 - export 403
 - external clock source
 - properties 88
 - external communication failure 465
 - external power down 478
 - external power down channels 1, 2 478
 - external power down channels 1, 2, 3, 4 476
 - external power down channels 3, 4 478
 - external power down channels 5, 6, 7, 8 476
 - external power down complete module 475
 - external power-down 477
 - external power-down complete module 479
- ## F
- fail-back 107, 289
 - fail-over 106, 289
 - failure 521, 524, 537
 - dangerous ~ 521
 - safe ~ 537
 - fault 525
 - loop ~ 473, 474, 475, 479
 - reaction 525
 - fault detection and response
 - behavior alarm markers 386
 - faults
 - first loop ~ 248
 - field
 - ~ status 394
 - file
 - ~ locations 13
 - ~
 - menu 44, 125, 144, 180, 229, 237, 243, 263
 - block ~ 218
 - equation ~ 188, 211
 - import ~ 195, 214
 - log ~ 227, 230, 237, 493
 - view ~ 193
 - find point 220
 - FLD 178
 - copy ~ 191
 - create ~ 190
 - layout 183
 - number 407
 - open ~ 189
 - properties 193
 - renumber ~ 193
 - FLD bar 183, 264

- flip-flops 378
- float 400
- force 268
 - clear all 269
 - disable fails 472
 - key switch 269
 - not successful 482
- forcing points 292
- forgotten password 284
- FSC 395
- FSC-FSC communication timeout 510
- FTE 78, 89, 111
- function block 209, 367
 - binary input 350
 - binary output 350
 - boolean input 350
 - boolean output 350
- function blocks 184
- Functional Block Diagram 8
- Functional Logic Diagrams 178
- functional logic diagrams different (OLM) 466
- functional safety 526
- functional safety assessment 528
- functions
 - compare 356
 - logical 353

G

- gateway address 80
- generate Logical View 53
- GPS 336
- GPS clock 292
- greater than gate 356
- greater than or equal gate 357

H

- Hardware Configurator 128
- hardware safety integrity 528
- high demand mode of operation 531, 539
- historical diagnostics 249
- human error 528

I

- I/O allocation error 497

- idle state initiated due to online modification 471
- IEC 61508 5
- IEC 61511 5
- IEEE 1588 335
- illegal argument, e.g. square root of -1 466
- illegal command 481
- illegal counter value (0 .. 8191) 466
- illegal timer value (0 .. 2047) 466
- import 403
- incompatible Safety Builder version 466
- input compare error 473
- installation 15
 - necessities 15
 - procedure 16
 - uninstallation 20
- integer 400
- interaction 32
- interface configuration 274
- internal power-down 474, 475
- inverter 355
- IO chassis properties 137
- IO symbols 347
- IO-0001
 - configuration error 480
 - error code not defined 480
 - module faulty 480
- IP address 78, 80, 89, 111

J

- justification 276

K

- key switch cycled from RUN to IDLE 471
- keyboard 32

L

- ladder diagram 8
- lead breakage 475
- less than gate 357
- less than or equal gate 357
- license 15
 - agreement 17
 - number 17
- line monitor circuit faulty 479

- link
 - ~ status report 256, 258
- link status report
 - communication ~ 256, 258
- load
 - Controller file 251
- location 394
- logical functions 206, 353
- logical link 287
- logical network 291
- Logical View 50
 - generate 53
- long 400
- long word 400
- loop fault
 - analog ~ 473, 474
 - digital ~ 475, 479
 - first ~ 248
- loop monitoring 251, 387
- lost password 284
- low demand mode of operation 531, 538

M

- markers
 - alarm 381, 385
 - diagnostic 381
 - reset 381, 384
 - state 386
 - system 381, 382
- master 319
- master ~ 530
- master/slave communication 288
- mathematical operations 360
- Maximum
 - Response time 505
- maximum repair time 134
- memory error 471
- menu bar 28
- messages
 - actual output status invalid 475, 476, 477
 - analog input loop fault 473, 474
 - application configuration has been modified... 481
 - application execution time failure 467
 - application program corrupted 470
 - BKM transport switch off or fuse blown 472
 - calculation overflow 464

- Check battery 472
- Check VDC power supply voltage 464
- clear not successful 481
- com module inserted 471
- com module removed 471
- communication module faulty 471
- configuration error 480
- Control Processor halt 470
- Controller not loaded 470
- Controller not running or application configuration different from loaded application 481
- correlation between channels 478
- CP-CP incompatible Point allocation 470
- current detected in output loop 478
- diagnostics 461
- divide by zero 465
- earth fault detected 474
- embedded software corrupted 470
- error code not defined 465, 480
- ESD input activated 465
- execution time out of range 470
- external communication failure 465
- external power down 478
- external power down channels 1, 2 478
- external power down channels 1, 2, 3, 4 476
- external power down channels 3, 4 478
- external power down channels 5, 6, 7, 8 476
- external power down complete module 475
- external power-down 477
- external power-down complete module 479
- force disable fails 472
- force not successful 482
- functional logic diagrams different (OLM) 466
- idle state initiated due to online modification 471
- illegal argument, e.g. square root of -1 466
- illegal command 481
- illegal counter value (0 .. 8191) 466
- illegal timer value (0 .. 2047) 466
- incompatible Safety Builder version 466
- input compare error 473
- internal power-down 474, 475
- key switch cycled from RUN to IDLE 471
- lead breakage 475
- line monitor circuit faulty 479
- memory error 471

- module
 - faulty 472, 473, 474, 475, 476, 477, 478, 479, 480
 - module faulty, voltage monitoring channel 474
 - no connection 481
 - no differences between applications 467
 - open loop or line monitor circuit faulty 479
 - output channel cannot be switched off 476, 477, 478, 479
 - output channel cannot be switched on 479
 - output compare
 - error 476, 477, 478, 479, 480
 - output is incorrectly switched on 479
 - output short circuit 476, 477, 478, 480
 - Point not found 482
 - power supply to field device shorted 467
 - processor module key in IDLE position 467
 - QPP display 458
 - repair timer expired 468
 - repair timer started 468
 - safe state initiated by other CP 468
 - safe state initiated by software assertion 468
 - secondary switch off asserted 469
 - short-circuits 475
 - spurious watchdog interrupt 469
 - temperature pre-alarm 469
 - temperature sensor faulty 471
 - temperature shutdown 469
 - the application can not be viewed... 482
 - timeout while retrieving status of the Controller 482
 - unable to initialize dynamic arrays for point and line data 482
 - unable to initialize the status of FLD 482
 - unable to start Application Viewer 482
 - voltage output short circuit or module faulty 474
- messages (diagnostics) 462
- mode of operation 531, 538, 539
 - continuous ~ 531, 539
 - high demand ~ 531, 539
 - low demand ~ 531, 538
- module
 - properties 139
- module
 - faulty 472, 473, 474, 475, 476, 477, 478, 479, 480
- module faulty, voltage monitoring channel 474
- modules 131

- add ~ 131
- mouse 35
- move
 - chassis 131
 - component 59
 - symbol 217
- multidrop link 288
 - master/slave 288
- multiple binary off-sheet transfer 352
- multiple boolean off-sheet transfer 352
- multiply gate 359

N

- NAND 353
- natural logarithm gate 361
- network
 - physical 49
- Network Configurator 42
- networks 287, 288, 289, 319, 320, 325
 - logical link 287
 - master 319
 - master/slave 288
 - multidrop link 288
 - redundant link 289
 - slave 319
 - system numbers 320
 - time-out time 325
- no connection 481
- no differences between applications 467
- nodes
 - expand ~ 56
- non-functional symbols 380
- NOR 354
- not equal gate 356
- NTP 335
 - ~3 335
 - ~4 335
- NTP protocol 292
- numeric 400

O

- on-line tools 11
- open FLD 189
- open loop 387
- open loop or line monitor circuit faulty 479
- options 274

- OR 354
- outlook bar 29
- output channel cannot be switched
 - off 476, 477, 478, 479
- output channel cannot be switched on 479
- output compare error 476, 477, 478, 479, 480
- output is incorrectly switched on 479
- output short circuit 476, 477, 478, 480

P

- packaged coils 314
- packages 10
 - basic ~ 10
 - contractor ~ 10
 - demo ~ 10
- password 281
 - active period 274, 284
 - change ~ 283
 - enter ~ 282
 - forgotten ~ 284
- paste 32
- PCDI 303
- Peer Control Data Interface 303
- physical network 49, 291
 - properties 90
- Physical View 50
- plant 48
 - properties 72
- plant clock 292
- point 141
 - ~ database 162
 - attributes 160
 - find ~ 220
 - importing and exporting ~s 162
 - properties 167
 - SafeNet allocation 324
 - type ~ 393
- Point Configurator 141
- Point not found 482
- power supply to field device shorted 467
- power-up 399
- prerequisite skills 4
- Process Under Control (PUC) 5
- processor module key in IDLE position 467
- Programmable Electronic System (PES) 534
- properties
 - CEE Controller ~ 85

- DCS ~ 87
- Experion Server ~ 86
- Experion server ~ 86
- external clock source ~ 88
- module ~ 139
- physical network ~ 90
- plant ~ 72
- point 167
- Safety Builder ~ 74
- set ~ 60
- SM Controller ~ 75
- view ~ 60

- PTP 335
- PTP protocol 292
- pulse 371
- Pulse timer 371

Q

- QPP display messages 458
- QPP-0001
 - application program corrupted 470
 - Control Processor halt 470
 - Controller not loaded 470
 - CP-CP incompatible Point allocation 470
 - embedded software corrupted 470
 - execution time out of range 470
 - idle state initiated due to online
 - modification 471
 - key switch cycled from RUN to IDLE 471
 - memory error 471
 - temperature sensor faulty 471
 - temperature shutdown 469

R

- range 400
 - analog output 349
 - calculation ~ 216, 358
 - constant 365
 - counter 362
 - float 269
 - node address 77, 108
 - scale 70, 224
 - tools ~ 11
- read 403
- real 400
- real time ~ 83
- real-time clock

- accuracy 315, 326
- synchronization 316, 327
- redo 32
- redundant link 289
- register 363
 - type 400
- registers
 - alarm 386
 - system 383
- remote reset 381, 384
- remove 20
- remove Safety Builder 20
- rename cabinet 130
- rename component 60
- renumber FLD 193
- repair timer 536
- repair timer expired 468
- repair timer started 468
- report
 - communication link status ~ 256, 258
- reset
 - marker 381, 384
 - remote ~ 381, 384
- Response time 505
- response time 324
- restore 64
- revision cloud 380
- risk 536
- RO-1024
 - error code not defined 480
 - output compare error 480
- RS232 291
- RS422 291
- RS485 291

S

- safe failure 537
- safe state initiated by other CP 468
- safe state initiated by software assertion 468
- SafeNet communication 288
 - master/slave 288
 - multidrop link 288
- safenet protocol 291
- safety 526, 537
 - functional ~ 526
- Safety Builder 48

- install ~ 15
- properties 74
- remove ~ 20
- tools 41, 239, 271
- uninstall ~ 20
- Safety Builder messages
 - application configuration has been modified... 481
 - clear not successful 481
 - Controller not running or application configuration different from loaded application 481
 - force not successful 482
 - illegal command 481
 - no connection 481
 - Point not found 482
 - the application can not be viewed... 482
 - timeout while retrieving status of the Controller 482
 - unable to initialize dynamic arrays for point and line data 482
 - unable to initialize the status of FLD 482
 - unable to start Application Viewer 482
- Safety Builder protocol 292
- Safety Instrumented Function (SIF) 5
- Safety Instrumented System (SIS) 5
- safety integrity 528, 544
 - hardware ~ 528
 - systematic ~ 544
- Safety Integrity Level (SIL) 5
- safety life cycle 540
- Safety related 540
- Safety-related 396
- safety-related system 540
- SAI-0410
 - analog input loop fault 473
 - input compare error 473
 - module faulty 474
 - voltage output short circuit or module faulty 474
- SAI-1620m
 - analog input loop fault 474
 - internal power-down 474
 - module faulty 474
 - module faulty, voltage monitoring channel 474
- SAO-0220m
 - actual output status invalid 476
 - module faulty 476

- output compare error 476
- satellite 336
- scaling 400
- SDI-1624
 - input compare error 473
 - module faulty 473
- SDI-1648
 - input compare error 473
 - module faulty 473
- SDIL-1608
 - earth fault detected 474
 - internal power-down 475
 - lead breakage 475
 - module faulty 475
 - short-circuits 475
- SDO-04110
 - actual output status invalid 477
 - external power-down 477
 - module faulty 477
 - output channel cannot be switched off 477
 - output compare error 477
 - output short circuit 477
- SDO-0424
 - actual output status invalid 477
 - external power down 478
 - external power down channels 1, 2 478
 - external power down channels 3, 4 478
 - module faulty 478
 - output channel cannot be switched off 478
 - output compare error 478
 - output short circuit 478
- SDO-0448
 - actual output status invalid 477
 - external power-down 477
 - module faulty 477
 - output channel cannot be switched off 477
 - output compare error 477
 - output short circuit 477
- SDO-0824
 - actual output status invalid 475
 - external power down channels 1, 2, 3, 4 476
 - external power down channels 5, 6, 7, 8 476
 - external power down complete module 475
 - module faulty 476
 - output channel cannot be switched off 476
 - output compare error 476
 - output short circuit 476
- SDOL-0424
 - correlation between channels 478
 - current detected in output loop 478
 - external power-down complete module 479
 - line monitor circuit faulty 479
 - module faulty 479
 - open loop or line monitor circuit faulty 479
 - output channel cannot be switched off 479
 - output channel cannot be switched on 479
 - output compare error 479
 - output is incorrectly switched on 479
 - output short circuit 480
 - secondary switch off asserted 469
 - Secondary switch-off
 - Digital I/O allocation error 497
 - When mandatory? 497
 - security 281
 - serial number 17
 - set privilege window 282
 - set properties 60
 - sheet transfers 204, 351
 - short 387
 - short-circuits 475
 - shortcut keys 32
 - signal conversion 366
 - signal type 400
 - SIL 395
 - single line 346
 - size 402
 - slave 319
 - slots 131, 403
 - SM Controller 48
 - properties 75
 - SM controller
 - copy ~ 62
 - enable remote load 64
 - migrating ~s 62
 - selecting a ~ 61
 - set ~ loaded 64
 - SMOD 542
 - SOE 292
 - spurious watchdog interrupt 469
 - square gate 360
 - square root gate 360
 - start configuration 56
 - states
 - Control Processor 520
 - IO 530
 - process 534
 - statistics

- communication ~ 256, 257
- status 387, 394
 - communication ~ 256, 257
 - communication link ~ report 256, 258
- status bar 31
- stop configuration 56
- structured text 8
- subnet mask 80
- subtract gate 358
- subunit 395
- symbol 216
 - change ~ 218
 - copy ~ 217
 - delete ~ 218
 - drag ~ 217
 - move 217
 - non-functional 380
 - properties 218
- SYS 395
- system information 253
- System Views 149
- systematic safety integrity 544
- systems 288
 - master/slave 288

T

- tag number 394
- temperature pre-alarm 469
- temperature sensor faulty 471
- temperature shutdown 469
- temporary connect 247
- text 380
- textual languages 8
- the application can not be viewed... 482
- third party software 18
- time
 - cycle ~ 324
 - response 324
 - time-out 324
- time server 335
- time synchronization 260
- time zone 74, 86, 88, 106, 333, 443, 447
- Timeout inconsistency 510
- time-out time 324
- timeout while retrieving status of the Controller 482

- Timeouts
 - FSC-FSC communication ~ 510
- time-outs 325
 - networks 325
- timer base 375, 407
- timer value 375, 408
- timers 215, 371
- token 106, 289
- tool bar 30
- tools 11, 41, 239, 271
 - Application Compiler 226
 - Application Editor 178
 - Application Viewer 261
 - Audit Trail 276
 - Controller Management 240
 - Hardware Configurator 128
 - Network Configurator 42
 - on-line ~ 11
 - Point Configurator 141
- top scale 401
- transfer 204
 - binary off-sheet ~ 352
 - binary on-sheet ~ 351
 - boolean off-sheet ~ 351
 - boolean on-sheet ~ 351
 - multiple binary off-sheet ~ 352
 - multiple boolean off-sheet ~ 352

U

- unable to initialize dynamic arrays for point and line data 482
- unable to initialize the status of FLD 482
- unable to start Application Viewer 482
- undo 32
 - maximum 274
- uninstall Safety Builder 20
- uninstallation 20
- unit 395
- USI-0001
 - com module inserted 471
 - com module removed 471
 - communication module faulty 471
 - module faulty 472

V

- validation 545

- view properties 60
- Views 50
 - System 149
- views 148
- voltage output short circuit or module faulty 474

W

- warnings
 - diagnostic messages 461
- warnings (diagnostic messages) 462
- word 400
 - long ~ 400
- work area 28
- write 403
- write enable 399
- WriteAlways 306
- WriteOnChange 306
- WriteOnDiff 306

X

- XNOR 355
- XOR 354

Fax Transmittal

Fax Number: +31 (0)73 6219 125

Reader Comments

To: Honeywell Safety Management Systems, attn. Technical Documentation Group

| | | |
|-------|------------|-------------|
| From: | Name: | Date: |
| | Title: | |
| | Company: | |
| | Address: | |
| | City: | State: Zip: |
| | Telephone: | Fax: |

Safety Manager Software Reference, Release 131, Issue 1, 20 February 2008

Comments:

You may also call the Technical Documentation Group at +31 (0)73 6273 273,
email Honeywell SMS at sms-info@honeywell.com, or write to:

Honeywell Process Solutions
Safety Management Systems
P.O. box 116
5201 AC 's-Hertogenbosch
The Netherlands

**Safety Manager
User documentation**

Honeywell

Honeywell Process Solutions
Safety Management Systems
Rietveldenweg 32a
5222 AR 's-Hertogenbosch
The Netherlands